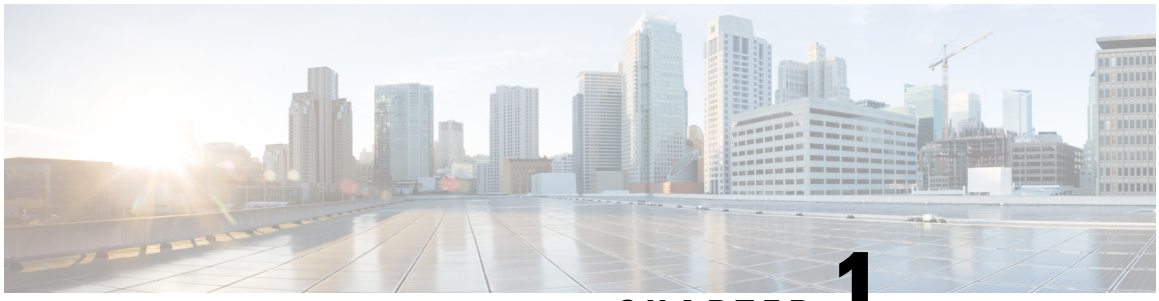
Cisco ACI Virtual Edge Installation Guide, Release 3.2(x)

First Published: 2021-06-08

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

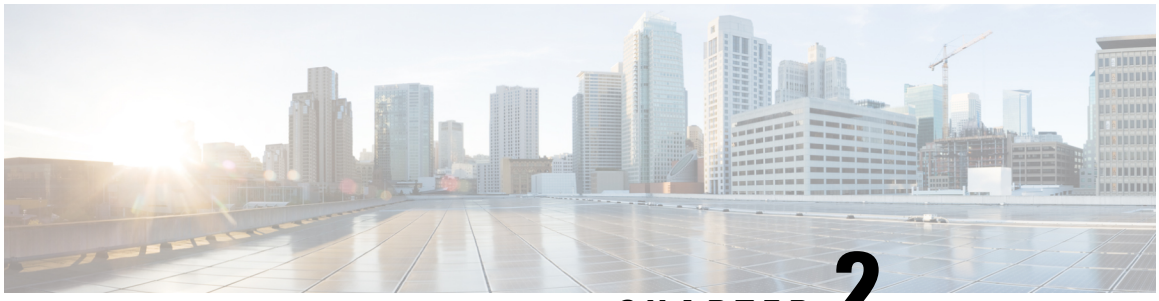
New and Changed Information

New and Changed Information

The following table provides an overview of the significant changes to this guide up to this current release.

Feature	Description	Were Documented
There are no new installation-related features in this release for Cisco ACI Virtual Edge.	This document has no changes from the previous release.	N/A

New and Changed Information



CHAPTER 2

Cisco ACI Virtual Edge

This chapter contains the following sections:

What Cisco ACI Virtual Edge Is

Beginning with the Cisco APIC Release 3.1(1), the Cisco Application Centric Infrastructure (ACI) supports the Cisco ACI Virtual Edge. Cisco ACI Virtual Edge is the next generation of the Application Virtual Switch (AVS) for Cisco ACI environments. Cisco ACI Virtual Edge is a hypervisor-independent distributed service VM that leverages the native distributed virtual switch that belongs to the hypervisor. Cisco ACI Virtual Edge runs in the user space, operates as a virtual leaf, and is managed by the Cisco Application Policy Infrastructure Controller (APIC).

If you use Cisco AVS, you can migrate to Cisco ACI Virtual Edge; if you use VMware VDS, you can run Cisco ACI Virtual Edge on top of it. Decoupling the Cisco ACI Virtual Edge from the kernel space makes the solution adaptable to different hypervisors. It also facilitates simple upgrades as Cisco ACI Virtual Edge is not tied to hypervisor upgrades. Cisco ACI Virtual Edge implements the OpFlex protocol for control plane communication. It supports two modes of traffic forwarding: local switching and no local switching.

Cisco ACI Virtual Edge Release 1.1(1a) supports only the VMware hypervisor. It leverages the vSphere Distributed Switch (VDS), which is configured in private VLAN (PVLAN) mode.

When network administrators create a Cisco ACI Virtual Edge VMM domain on Cisco APIC, they must associate the domain with a range of VLANs to be used for PVLAN pair association of port groups on the DVS. Server administrators do not need to associate PVLANs to port groups on vCenter because Cisco APIC automatically associates PVLAN pairs with the endpoint groups (EPGs).

Note EPGs in Cisco APIC are equivalent to port groups in vCenter.

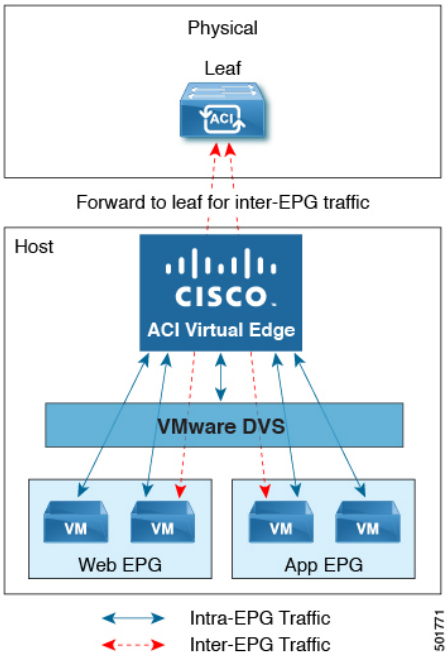
Local Switching Mode

In Local Switching mode, the Cisco ACI Virtual Edge locally forwards all intra-EPG traffic without involving the leaf. All inter-EPG traffic is forwarded through the leaf. In this mode, the Cisco ACI Virtual Edge can use either VLAN or VXLAN encapsulation—or both—for forwarding traffic to the leaf and back. You choose the encapsulation type during Cisco ACI Virtual Edge VMM domain creation.

You can configure a single VMM domain in Local Switching mode to use VLAN and VXLAN encapsulation.

If you choose VLAN encapsulation, a range of VLANs must be available for use by the Cisco ACI Virtual Edge. These VLANs have local scope in that they have significance only within the Layer 2 network between the Cisco ACI Virtual Edge and the leaf. If you choose VXLAN encapsulation, only the infra-VLAN must be available between the Cisco ACI Virtual Edge and the leaf. This results in a simplified configuration. It is the recommended encapsulation type if there are one or more switches between the Cisco ACI Virtual Edge and the physical leaf.

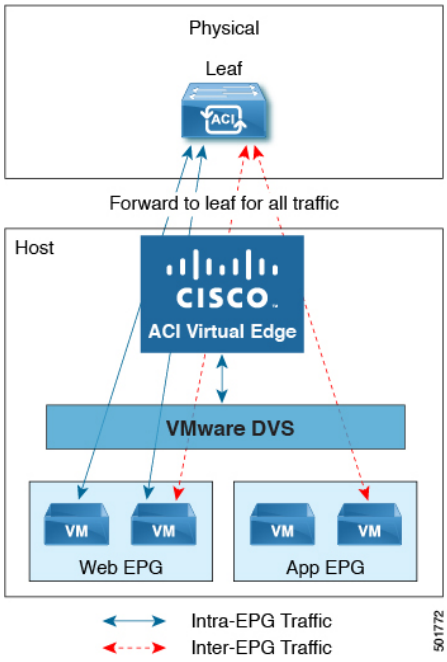
Figure 1: The Cisco ACI Virtual Edge in Local Switching Mode



No Local Switching Mode

In No Local Switching mode, the leaf forwards all traffic. In this mode, VXLAN is the only allowed encapsulation type.

Figure 2: The Cisco ACI Virtual Edge in No Local Switching Mode



Statistics Collection

Statistics collection is enabled on Cisco ACI Virtual Edge by default. You may see Cisco ACI Virtual Edge faults within the Cisco APIC GUI relating to VM resource use.

Troubleshoot those faults in the VMware vCenter because the Cisco ACI only generates these faults based on information it receives from VMware vCenter.

Cisco ACI Virtual Edge and the VMware vCenter

The Cisco ACI Virtual Edge is a distributed virtual switch that extends across many virtualized hosts. It manages a data center defined by the vCenter Server.

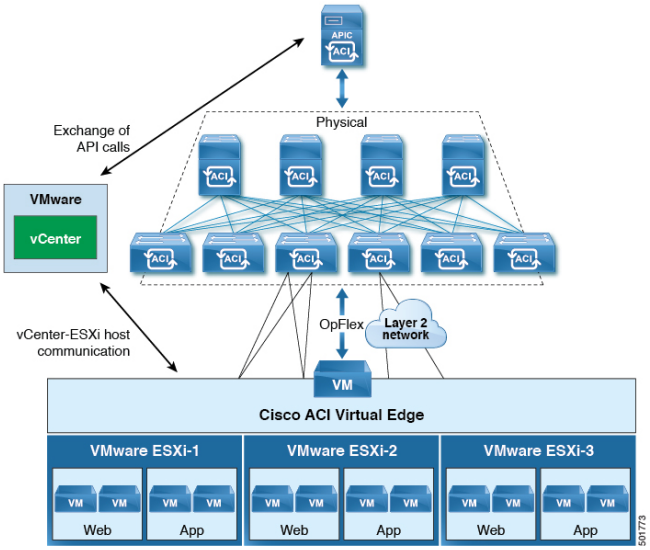
The Cisco ACI Virtual Edge is compatible with any upstream physical access layer switch that complies with the Ethernet standard, including Cisco Nexus switches. The Cisco ACI Virtual Edge is compatible with any server hardware listed in the *VMware Hardware Compatibility List* (HCL).

The Cisco ACI Virtual Edge is a distributed virtual switch solution that is fully integrated within the VMware virtual infrastructure, including VMware vCenter for the virtualization administrator. This solution allows the network administrator to configure virtual switch and port groups in order to establish a consistent data center network policy.

Note VMs deployed on Cisco ACI Virtual Edge support physical MAC addresses as indicated by vCenter; virtual MAC addresses are not supported.

The following figure shows a topology that includes the Cisco ACI Virtual Edge with the Cisco APIC and VMware vCenter.

Figure 3: Sample Cisco ACI Virtual Edge Topology



Note If there are multiple vCenters connected to a single Cisco ACI fabric, you should ensure that there are no overlapping MAC address allocation schema across the multiple vCenters while deploying the vCenters instead of the default OUI allocation. Overlaps can cause duplicate MAC address generation. For more information, see VMware documentation.

Cisco ACI Virtual Edge in a Multipod Environment

The Cisco ACI Virtual Edge can be part of a multipod environment. Multipod environments use a single Cisco APIC cluster for all the pods; all the pods act as a single fabric.

Multipod environments enable a more fault tolerant fabric comprising multiple pods with isolated control plane protocols. They also provide greater flexibility in full mesh cabling between leaf and spine switches.

Cisco ACI Virtual Edge does not require any additional configuration to operate in a multipod environment.

For detailed information about multipod environments, see the following documents on Cisco.com:

- *Cisco Application Centric Infrastructure Fundamentals*
- *Cisco APIC Getting Started Guide*
- *Cisco APIC NX-OS Style Command-Line Interface Configuration Guide*

The following features are not supported for Cisco ACI Virtual Edge with multipod in Cisco APIC releases 3.1(1) through 4.0(1):

- Storage vMotion with two separate NFS in two separate PODs
- ERSPAN destination in different PODs

- Distributed Firewall syslog server in different PODs

Required Software

The following table shows the versions of software required for Cisco ACI Virtual Edge to work with the Cisco APIC, VMware vCenter, and VMware ESXi hypervisor:

Component	Description
Cisco ACI Virtual Edge software	Cisco ACI Virtual Edge is supported beginning with Release 1.1(1).
Cisco APIC	Cisco ACI Virtual Edge is supported in Cisco APIC beginning with Release 3.1(1).
VMware vCenter	Cisco ACI Virtual Edge is compatible with release 6.0 and later versions of VMware vCenter Server.
VMware vSphere bare metal	Cisco ACI Virtual Edge is supported as a vLeaf for the Cisco APIC with release 6.0 and later releases of the VMware ESXi hypervisor.

Cisco ACI vPod: Extending the Cisco ACI Fabric

Organizations increasingly adopt hybrid data center models to meet infrastructure demands, flexibility, and reduce costs. They combine various technologies—including virtual private clouds and other internal IT resources—with remote locations. The remote locations can be hosted data centers, satellite data centers, or multicloud environments.

However, hybrid deployments require consistent management and policy for workloads regardless of their location. They also require support for disaster recovery and the ability to migrate workloads between data centers. Meanwhile, they can lack compatible hardware or space to add new equipment.

By deploying Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod), you can overcome these challenges and virtually extend the Cisco ACI fabric into various remote locations.

What Cisco ACI vPod Is

Cisco ACI vPod was introduced with general availability in Cisco APIC Release 4.0(2). It is a software-only solution that you can deploy wherever you have at least two servers on which you can run the VMware ESXi hypervisor. Cisco ACI vPod and its components—a virtual spine (vSpine), virtual leaf (vLeaf), and Cisco ACI Virtual Edge, run on the ESXi hypervisor.

Cisco ACI vPod allows you to use Cisco ACI Virtual Edge where you do not have a physical leaf. You can use up to eight instances of Cisco ACI Virtual Edge in each Cisco ACI vPod in the remote location as you would in your on-premises data center.

Cisco ACI vPod communicates with a physical, on-premises pod or multipod over an interpod network (IPN). You configure the physical pod or multipod, the IPN connection, and Cisco ACI vPod in Cisco Application Policy Infrastructure Controller (APIC). You then use the Cisco ACI vCenter plug-in, a Python script, or PowerCLI to deploy Cisco ACI vPod components.

Benefits of Cisco ACI vPod

Once Cisco ACI vPod is installed, you can use it with Cisco APIC to enforce Cisco ACI fabric policy in the remote location.

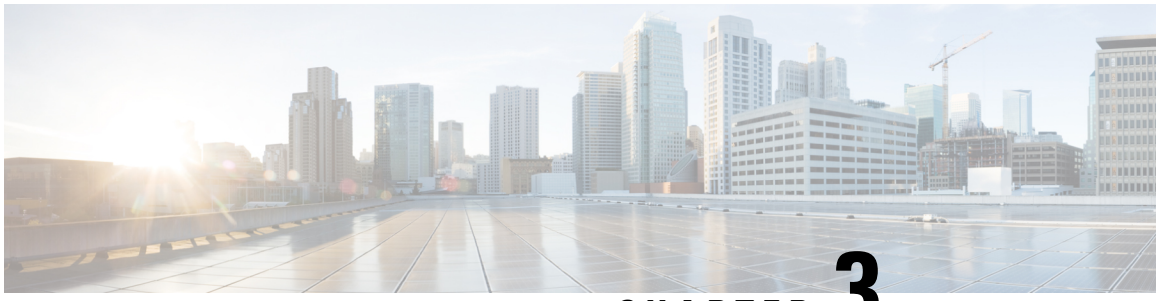
Cisco APIC provides central management of workloads in the on-premises data center and the remote location. It enables you to enforce policy easily and consistently in both on-premises and remote locations.

The flexibility, scalability, and central management of the Cisco ACI vPod solution enable you to take advantage of the following use case scenarios:

- Extension of the Cisco ACI fabric to the bare-metal cloud
- Extension of the Cisco ACI fabric to brownfield deployments
- Extension of the Cisco ACI fabric to colocation data centers
- Migration of workloads from non-Cisco hardware to the Cisco ACI fabric

Where to Find More Information

For general information, see the *Cisco ACI Virtual Pod Release Notes* on Cisco.com.



CHAPTER 3

Cisco ACI Virtual Edge Installation

This chapter describes installation for Cisco ACI Virtual Edge, including prerequisites and installation methods.

About Cisco ACI Virtual Edge Installation

Cisco ACI Virtual Edge installation consists of a series of tasks on the Cisco APIC, and VMware vCenter. You can then use one of three methods to deploy Cisco ACI Virtual Edge on ESXi hosts:

- Cisco ACI vCenter plug-in
- VMware PowerCLI (for Windows platforms)
- Python script

Note Do not use the vSphere (thick) Client to install Cisco ACI Virtual Edge or modify its vApp properties. Use only the Cisco ACI vCenter plug-in, the VMware Power CLI, or a Python script to install Cisco ACI Virtual Edge. Use only the vSphere Web Client to modify Cisco ACI Virtual Edge vApp properties.

Note When you deploy the Cisco ACI Virtual Edge VM on the ESXi hosts, OpFlex automatically comes online. Do not attach VMkernel ports to the Infra port group, as was done for OpFlex for Cisco AVS.

The following sections provide information about prerequisites and installation methods. For information about migrating from Cisco AVS to Cisco ACI Virtual Edge, see the chapter Migration from Cisco AVS to Cisco ACI Virtual Edge, on page 41 in this guide. For information about migrating from VMware VDS to Cisco ACI Virtual Edge, see the chapter Migration from VMware VDS to Cisco ACI Virtual Edge, on page 49 in this guide.

Note Although you can install multiple Cisco ACI Virtual Edge VMs on the same host (one for each Cisco ACI Virtual Edge VMM domain), we recommend that you install only one Cisco ACI Virtual Edge VM per host.

Best Practices for Cisco ACI Virtual Edge Deployments

Follow these best practices to minimize traffic loss and provide more availability due to hardware failure.

- For ACI Virtual Edge deployments, ensure to configure ProActive HA in the cluster on vCenter, and on the VMM domain on APIC.
- For ProActive HA deployments for ACI Virtual Edge, ensure the DRS Setting on the vCenter to disable the For Availability, distribute a more even number of virtual machines across hosts option.

See the *Improving Cisco ACI Virtual Edge Availability with VMware vSphere Proactive HA* chapter, for more details about Enabling vSphere Proactive HA.

Default Port-Groups

When you create a Cisco Application Centric Infrastructure (ACI) Virtual Edge, VMware vCenter automatically creates several port-groups:

- **ave-external-vxlan-1 and ave-external-vxlan-2:** The Cisco ACI Virtual Edge virtual machine (VM) uses these port-groups to send and receive VXLAN traffic to and from outside the host. VXLAN traffic is distributed between these two ports based on the incoming VM interface.
- **ave-internal-1 and ave-internal-2:** The Cisco ACI Virtual Edge VM uses these port-groups to send and receive PVLAN traffic to and from VMs internal within the distributed virtual switch (DVS). The internal VLAN blocks are distributed evenly between these two port-grouups to load-balance the internal traffic.
- **ave-external-vlan:** The Cisco ACI Virtual Edge VM uses this port-group to send and receive VLAN traffic to and from outside the host. It enables the VLANs used for the VLAN mode endpoint groups (EPGs) associated with the VMM domain. The VLANs might include the VLAN assigned to "ave-ctrl" EPG, if it is in VLAN mode.
- **infra:** VMs use this special port-group to receive ERSPAN traffic originated from another Cisco ACI Virtual Edge. The port-group is in native mode, and incoming Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic bypasses Cisco ACI Virtual Edge and is forwarded by the DVS.

Cisco ACI Virtual Edge Installation Workflow

This section provides a high-level description of the tasks required to install the Cisco ACI Virtual Edge.

1. Fulfill all the prerequisites, which include tasks in the Cisco Application Policy Infrastructure Controller (APIC), and vCenter. See the section Prerequisites for Installing Cisco ACI Virtual Edge , on page 11.
2. Download the Cisco ACI Virtual Edge Open Virtualization Format (OVF) file from Cisco.com and then upload it to the vCenter content library. You can use the vCenter plug-in, the vCenter power CLI, or a Python script. See one of the following sections for instructions:
   - Upload the OVF File Using the Flash Version of the Cisco ACI vCenter Plug-in , on page 24
   - Setting Up the PowerCLI Environment, on page 28

     and Managing the VMware vCenter Content Library Using the VMware PowerCLI, on page 29
   - Setting Up the Python Environment, on page 32

     and Managing the VMware vCenter Content Library Using Python, on page 33
3. Deploy Cisco ACI Virtual Edge on the ESXi hosts. You can use one of three methods. See the following sections for instructions:
   - Deploy Cisco ACI Virtual Edge Using the Flash Version of the Cisco ACI vCenter Plug-In, on page 26
   - Deploying Cisco ACI Virtual Edge Using the VMware PowerCLI, on page 30
   - Deploying Cisco ACI Virtual Edge Using Python, on page 34
4. Make sure that the that the interface that is used to communicate with Cisco ACI Virtual Edge (kni0) has a virtual tunnel endpoint (VTEP) IP address and verify that OpFlex is up.

   See the section Verify the Cisco ACI Virtual Edge Deployment, on page 36 in this guide.

Note To ensure a higher level of availability, we recommend that you deploy Cisco ACI Virtual Edge on a local data store.

Prerequisites for Installing Cisco ACI Virtual Edge

Perform the following tasks before you install Cisco Application Centric Infrastructure Virtual Edge:

Storage and Memory

You need at least 30 GB of storage and 4 GB of memory.

Cisco ACI Fabric and Cisco APIC

- Make sure that Cisco Application Policy Infrastructure Controller (APIC) is set up correctly. See the *Cisco APIC Getting Started Guide* and *Cisco APIC Basic Configuration Guide*, on Cisco.com for instructions on how to configure Cisco APIC for the first time.
- Make sure that all switches are registered and that the Cisco ACI fabric is up-to-date. See *Cisco Application Centric Infrastructure Fundamentals* and the *Cisco APIC Getting Started Guide* on Cisco.com for instructions.

- Make sure that the Cisco ACI fabric is registered inside the vCenter plug-in. See "Connecting vCenter Plug-in to your ACI Fabric" in the chapter "Cisco ACI vCenter Plug-in" in the *Cisco ACI Virtualization Guide*.

VMM Domain

Create a new vCenter VMM domain and interface and switch profiles for Cisco ACI Virtual Edge.

We recommend that you use the unified configuration wizard to perform these tasks. See the procedure Create vCenter Domain, Interface, and Switch Profiles Using the GUI, on page 15 in this guide. However, you may need to configure separate, more detailed policies. If so, see the appendix Alternate Procedures for Creating vCenter Domain, Interface, and Switch Profiles, on page 75 in this guide.

Hosts

- Add one or more ESXi hosts and their PNICs to the new Cisco ACI Virtual Edge distributed virtual switch (DVS) in using vSphere Web Client on VMware vCenter.
- If the host belongs to a Distributed Resource Scheduler (DRS) cluster that already has VMs running on Cisco ACI Virtual Edge, put the host in maintenance mode before you add the Cisco ACI Virtual Edge DVS to it. Starting the installation with the host in maintenance mode prevents the DRS from migrating VMs to the other hosts before the Cisco ACI Virtual Edge VM is fully ready.
- If the host belongs to a DRS cluster, make sure that the Enhanced VMotion Compatibility (EVC) mode for the DRS cluster is set to Nehalem or higher.
- When using VMware vSphere Hypervisor (ESXi) 6.5 U1, update the Intel X710 port adapter driver to 1.8.6 or later with firmware 6.01 or later before adding hosts to the Cisco ACI Virtual Edge in VXLAN mode with Cisco Discovery Protocol (CPD) enabled. If you do not update the port adapter driver, you may see the VMware purple diagnostic screen.

VXLAN Encapsulation

When connecting the Cisco ACI Virtual Edge using VXLAN encapsulation, set the maximum transmission unit (MTU) value equal to or greater than 1600 on all intermediate devices on the path between the Cisco ACI fabric and the Cisco ACI Virtual Edge. These include FI switches and UCS-B. However, to optimize performance, set the MTU to the maximum supported size that all intermediate devices on the path between the Cisco ACI fabric and the Cisco ACI Virtual Edge support.

VMware vCenter

- In order to use the Cisco ACI Virtual Edge management tools, we recommend that you use vCenter 6.0 Update 3 or later. These tools include the ACI vCenter plug-in, the VMware PowerCLI, and Python scripts.
- If you plan to install Cisco ACI Virtual Edge using the VMware PowerCLI, synchronize the clocks for the vCenter Server, any Active Directory domain controllers, and the host making single-sign-on connection requests. If the clocks are not synchronized, you may encounter problems when deploying Cisco ACI Virtual Edge using the VMware PowerCLI tool.

  For details, see the knowledge base article "Calling the SSOConnection SDK reports the exception: Client received SOAP Fault from server: The time now <timestamp> does not fall in the request lifetime interval extended with clock tolerance of 600000 ms (2125193)" on the VMware website.

Remote Leaf Deployment

If you plan to install Cisco ACI Virtual Edge in a remote leaf deployment, enable **DSCP class-cos translation policy for L3 traffic** as recommended in the section "Recommended QOS configuration for Remote leaf" of the *Cisco ACI Remote Leaf Architecture White Paper* on Cisco.com.

Cisco APIC Settings Configuration

The following sections describe how to configure the Cisco ACI Virtual Edge and the VMware ESXi hypervisor with the Cisco APIC:

1. vCenter Domain, Interface, and Switch Profile Creation, on page 13
2. Interface and Switch Profile Guidelines and Prerequisites, on page 13
3. vCenter Domain Profile Guidelines and Prerequisites, on page 15
4. Create vCenter Domain, Interface, and Switch Profiles Using the GUI, on page 15

vCenter Domain, Interface, and Switch Profile Creation

Before you can install the Cisco ACI Virtual Edge, you must create vCenter domain, interface, and switch profiles. We recommend that you perform these tasks in the united configuration wizard in the Cisco APIC. See the procedure Create vCenter Domain, Interface, and Switch Profiles Using the GUI, on page 15 in this guide.

Understand and follow the guidelines in this section before proceeding with the tasks.

Alternate Procedures

If you want to configure a FEX profile or detailed interface, switch, or vCenter domain profiles, you can find instructions in Alternate Procedures for Creating vCenter Domain, Interface, and Switch Profiles, on page 75 in this guide.

Firewall Considerations

If you use the recommended united configuration wizard, the Cisco APIC automatically creates a firewall policy, which can be modified later. If you instead use the alternate procedures to create interface, switch, or vCenter domain profiles, you will need to create a firewall policy manually. Follow the instructions in the Distributed Firewall section of the Cisco ACI Virtual Edge Configuration Guide.

Interface and Switch Profile Guidelines and Prerequisites

Follow these guidelines and fulfill the prerequisites when creating interface and switch profiles for your Cisco ACI Virtual Edge.

Guidelines for Creating Interface and Switch Profiles

The Cisco ACI Virtual Edge supports port channel (PC), virtual port channel (VPC), MAC Pinning, and FEX interface policies.

- If there is a Layer 2 network between the leaf switch and the Cisco ACI Virtual Edge vSphere host, configure the interface policy on the interfaces that are connected to the Layer 2 network.

- The number of links and leafs that you use determine whether you configure a PC or a VPC policy for the Cisco ACI Virtual Edge:
  - If you are using multiple links between one leaf and an ESXi host, you must configure a PC policy.
  - If you are using multiple links between multiple leafs and an ESXi host, you must configure a VPC policy.
- Follow these guidelines for choosing a LACP policy:
  - Choose LACP (Active or Passive) if the uplinks from the Cisco ACI Virtual Edge (vSphere host) are directly connected to the leaf switches and you want to use or turn on the LACP channeling protocol.
  - Choose Static Channel - Mode On if the uplinks form the Cisco ACI Virtual Edge are directly connected to the leaf switches but you do not want to use the LACP channeling protocol.
  - Choose MAC Pinning if the uplinks from the Cisco ACI Virtual Edge will not be channeled together and will operate as separate links.

Note Do not use MAC pinning with a direct connection to a VPC leaf pair. Instead, use Link Aggregation Control Protocol (LACP) or enhanced LACP to provide redundancy and reliability. Using MAC pinning with a direct connection leads to traffic loss when peer leaf switches are rebooted. Use MAC Pinning only where virtual port channel (VPC) cannot be supported, such as for Cisco UCS Fabric Interconnects with southbound interfaces.

- Follow these guidelines for choosing a vSwitch port group for the management interface:

  Ensure that the vSwitch port group that you choose for the Cisco ACI Virtual Edge management interface can provide at least IPv4 addresses through DHCP or the vCenter IP pool. You can configure an additional IPv6 address for the vSwitch port group for the management interface; however, you cannot configure it only with an IPv6 address.

Note The Cisco ACI vCenter plug-in does not support configuration of a static IP address. However, you can configure a static IP address by using the VMware PowerCLI or Python script. See the sections Cisco ACI Virtual Edge Installation Using the VMware PowerCLI, on page 28 and Cisco ACI Virtual Edge Installation Using Python, on page 31 in this guide. Alternatively, you can configure a static IP address in VMware vCenter. See the section Configuring a Static IP Address in VMware vCenter, on page 39 or the section Configure a Static IP Address Using the HTML5 Version of the VMware vSphere Client, on page 38 in this guide.

Prerequisites for Creating Interface and Switch Profiles

Verify that the leaf switch interfaces are physically connected to the ESXi hypervisor. Or, if you are using a Layer 2 device, verify that the leaf is physically connected to the Layer 2 device.

vCenter Domain Profile Guidelines and Prerequisites

You must create a new vCenter domain profile before you can install Cisco ACI Virtual Edge. You cannot convert an existing vCenter domain profile.

Guidelines for Creating a VMware vCenter Domain Profile

You can create multiple data centers and DVS entries under a single domain. However, you can have only one Cisco ACI Virtual Edge assigned to each data center.

You can use IPv6 when creating a VMM domain if the vCenter and ESXi host management are IPv6-enabled.

Prerequisites for Creating a VMware vCenter Domain Profile

Ensure that the multicast IP address pool has enough multicast IP addresses. You must accommodate the number of EPGs to be published to the VMware vCenter domain. You can add more IP addresses to a multicast address pool that is already associated with a VMware vCenter domain at any time.

Ensure that you have enough VLAN IDs. If you do not, ports on endpoint groups (EPGs) might report that no encapsulation is available.

vCenter must be installed, configured, and reachable through the in-band/out-of-band management network.

You must have the administrator/root credentials to the vCenter.

Create vCenter Domain, Interface, and Switch Profiles Using the GUI

Note If you want to choose a delimiter for the VMware portgroup name when you create a vCenter domain, you cannot do so in this procedure. You also cannot use this procedure if you want to take advantage of the VMware vSphere Proactive HA feature. This procedure uses a configuration wizard that enables you to configure a vCenter domain, interface, and switch profiles.

Instead, you must create the vCenter domain separately. The delimiter option appears in the **Create vCenter Domain** dialog box. The **Create vCenter Domain** dialog box also includes an option to create a VMware Proactive HA object in VMware vCenter. It also includes an option to set the time periods before Proactive HA is triggered. See the procedure Create a VMM Domain Profile for Cisco ACI Virtual Edge , on page 82 in this guide.

Before you begin

Before you create a vCenter domain profile, you must establish connectivity to an external network using in-band management network on the Cisco APIC.

Procedure

Step 1 Log in to the Cisco APIC.

Step 2 On the menu bar, click **Fabric** > **Access Policies**.

Step 3 In the Policies **Navigation** pane, lick **Quick Start**, and then in the central pane, click **Configure Interfaces, PC, and VPC**.

Step 4 In the **Configure Interfaces, PC, and VPC** dialog box, expand **Configured Switch Interfaces**, click the green + icon, and then perform the following steps:

a) In the **Select Switches to Configure Interfaces** area, make sure that the **Quick** radio button is selected.

b) From the **Switches** drop-down list, choose the appropriate leaf ID.

In the **Switch Profile Name** field, the switch profile name automatically appears.

c) Click the green + icon again.

The **Configure Interfaces, PC, and VPC** dialog box displays a wizard that enables you to configure vCenter domain, interface, and switch profiles.

Step 5 In the wizard, perform the following actions:

a) In the **Interface Type** area, choose the appropriate radio button.

PC and VPC are the only valid options for Cisco ACI Virtual Edge deployment. See the section Interface and Switch Profile Guidelines and Prerequisites, on page 13 in this guide.

b) In the **Interfaces** field, enter the interface or interface range for your vSphere hosts.

Once you enter the interface or interface range, the wizard enters a name in the **Interface Selector Name** field.

c) In the **Interface Policy Group** area, choose the **Create One** radio button.

Note This procedure assumes that you are creating interface and switch policies and creating a vCenter domain rather than using existing ones. If you choose the **Choose One** radio button, you will not be able to create policies in the wizard.

d) From the **CDP Policy** or the **LLDP Policy** drop-down list, create a policy.

Note
- If you use a Cisco Unified Computing System (UCS) server, create two policies. Create one policy to enable a Cisco Discovery Protocol (CDP) policy and a second policy to disable Link Layer Discovery Protocol (LLDP).
- CDP and LLDP policies are disabled by default. You can enable them in the configuration wizard. Enable CDP or LLDP policies in the **Interface Policy Group** area to enable them on Cisco ACI Virtual Edge and other switches in the fabric. If you want to enable CDP or LLDP only on Cisco ACI Virtual Edge, enable them in the **vSwitch Policy** area of the configuration wizard.

e) From the **Link Level Policy** drop-down list, choose a link level policy or create one.

The link level policy specifies the speed of the physical interface. If you do not choose a link level policy, the speed defaults to 10 Gbps.

f) In the **Port Channel Policy** drop-down list, choose **Create Port Channel Policy**.

g) In the **Create Port Channel Policy** dialog box, enter a name for the policy, choose a mode, and then click **Submit**.

Choose the same policy mode that is on the ESXi server. For example, if the server does not support LACP, you can choose **Static Channel - Mode On** or **MAC Pinning**. Other fields in the dialog box are optional.

h) In the **Attached Device Type** area, choose **AVE VLAN Hosts** or **AVE VXLAN Hosts**.

Note If the hypervisors are directly connected to leaf switches, you can use either VLAN or VXLAN. (Cisco UCS blade servers, where Fabric Interconnects are connected to the fabric, are considered to be directly connected.) However, if the hypervisors are not directly connected to leaf switches, you must use VXLAN. For more information, see the Cisco ACI Virtual Edge, on page 3 section.

i) In the **Domain** area, make sure that the **Create One** radio button is chosen.

Use the **Create One** option to create a new VMM domain for an interface or switch profile, as you do in this procedure. Use the **Choose One** button to create an interface or switch profile for a new host that you want to make part of an existing VMM domain.

j) In the **Domain Name** field, enter the domain name.

Note When you create the VMM domain, you choose VLAN or VXLAN encapsulation, depending on the attached device type that you chose in Step 5 h. However, you can configure a single VMM domain to use VLAN and VXLAN encapsulation. After you finish installing the Cisco ACI Virtual Edge, you can enable mixed encapsulation mode. See the section "Mixed-Mode Encapsulation Configuration" in the Cisco ACI Virtual Edge Configuration Guide.

k) Complete one of the following series of steps:

Mandatory: If you use Cisco ACI Virtual Edge and you deploy it in mixed-mode or VLAN mode, create a single VLAN pool with two VLAN encapsulation blocks. One will be used for primary encapsulation, and one will be used for private VLAN implementation.

If in Step 5 h you chose...	Then...
AVE VLAN Hosts	**1.** In the **VLAN** area, make sure that the **Create One** radio button is chosen. **2.** In the **VLAN Range** field, enter the VLAN range as appropriate. **Note** Do not define a range that includes the reserved VLAN ID for the infrastructure network because that VLAN is for internal use. The VLAN range is for external or on-the-wire encapsulations. It is used for allocating VLANs for each EPG assigned to the domain. The VLANs are used when packets are sent to or from leafs. **3.** In the **Internal VLAN Range** field, enter a range. The internal VLAN range is used for private VLAN allocations in the internal vSwitch by the Cisco ACI Virtual Edge. The VLANs are not seen outside the ESX host or on the wire. **Note** If you use Cisco ACI Virtual Edge and you deploy it in mixed-mode or VLAN mode, create a single VLAN pool with two VLAN encapsulation blocks. One will be used for primary encapsulation, and one will be used for private VLAN implementation.

If in Step 5 h you chose...	Then...
AVE VXLAN Hosts	**1.** In the **VLAN** area, make sure that the **Create One** radio button is chosen. **2.** In the **Internal VLAN Range** field, enter a range. **3.** In the **Fabric Multicast Address** field, enter a multicast address, such as 225.1.1.1. **4.** In the **Pool of Multicast Address Ranges** field, create a new multicast pool or choose an existing one. **Note** The multicast address that is configured in Step 3 must not overlap with the ranges that are configured in Step 4. **5.** In the **Local Switching** area, choose **True** or **False**. With local switching, traffic within an EPG does not go to the leaf. So if you choose local switching, you may not see some traffic counters. If you want to see all intra-EPG traffic, choose.**False** See the section What Cisco ACI Virtual Edge Is, on page 3 for additional information about Local Switching and No Local switching modes.

l) (Optional) From the **Security Domains** drop-down list, choose or create a security domain.
m) In the **vCenter Login Name** field, enter the vCenter Administrator/root username.
n) In the **Password** field, enter the vCenter Administrator/root password.
o) In the **Confirm Password** field, reenter the password.

Step 6 Click the + icon to expand **vCenter**, and in the **Create vCenter Controller** dialog box, perform the following actions:

Note You can create multiple vCenter controllers in the same domain. If you want to create more vCenter controllers, repeat the substeps for step 6 for each new vCenter controller.

a) In the **Name** field, enter a name to refer to the vCenter domain.

The name does not need to be the same as the vCenter domain name; you can use the vCenter hostname.

b) In the **Host Name (or IP Address)** field, enter the host name or IP address.

If you use the hostname, you must already have configured a DNS policy on Cisco APIC. If you do not have a DNS policy configured, enter the IP address of the vCenter server.

c) From the **DVS Version** drop-down list, choose a DVS version.

The DVS version that you choose represents the minimum ESXi version of the host that you can add to the virtual switch. So if you choose DVS version 6.0, you can add or manage hosts of ESXI version 6.0 and later.

Note Cisco ACI Virtual Edge supports DVS and ESXi versions 6.0 and later.

d) In the **Datacenter** field, enter the data center name.

The name that you enter for **Datacenter** must match exactly the name in vCenter. The name is case-sensitive.

e) Click OK.

Note For the following three steps, if you do not specify port channel, vSwitch, or interface control policies, the same interface policy that you configured earlier in this procedure will take effect for the vSwitch.

Step 7 In the **Configure Interface, PC, And VPC** dialog box, from the **Port Channel Mode** drop-down list, choose a mode.

Note
- Choose **MAC Pinning** if you have a Unified Computing System (UCS) Fabric Interconnect (FI) between the top-of-rack switch and the Cisco ACI Virtual Edge.
- Do not use MAC pinning with a direct connection to a VPC leaf pair. Instead, use Link Aggregation Control Protocol (LACP) or enhanced LACP to provide redundancy and reliability. Using MAC pinning with a direct connection leads to traffic loss when peer leaf switches are rebooted. Use MAC Pinning only where virtual port channel (VPC) cannot be supported, such as for Cisco UCS Fabric Interconnects with southbound interfaces.

Step 8 In the **vSwitch Policy** area, choose a policy.

Step 9 In the **Interface Controls** area, choose **BPDU Guard**, **BPDU Filter**, or both.

See the section "BPDU Features" in the Cisco ACI Virtual Edge Configuration Guide for information about BPDU Guard and BPDU Filter.

Step 10 From the **Firewall** drop-down list, choose **Learning**, **Enabled** or **Disabled** mode.

Learning mode, the default, should be used only when upgrading to Cisco ACI Virtual Edge from a version of Cisco AVS that does not support Distributed Firewall. Otherwise, Distributed Firewall should be in Enabled mode. You can change the Distributed Firewall mode later. See the chapter "Distributed Firewall" in the Cisco ACI Virtual Edge Configuration Guide.

Step 11 Disregard the NetFlow Exporter Policy option.

Step 12 Click **Save**, click **Save** again, and then click **Submit**.

Step 13 Verify the new domain and profiles, by performing the following actions:

a) On the menu bar, choose **Virtual Networking** > **Inventory**.

b) In the navigation pane, expand **VMM Domains** > **VMware** > ***Domain_name*** > **Controllers**, and then choose the vCenter.

In the work pane, under **Properties**, view the virtual machine manager (VMM) domain name to verify that the controller is online. In the work pane, the vCenter properties are displayed including the operational status. The displayed information confirms that connection from the Cisco APIC to the vCenter server is established, and the inventory is available.

Add ESXi Hosts and PNICs Using the VMware vSphere Client HTML5 GUI

Before you can install Cisco Application Centric Infrastructure (ACI) Virtual Edge, you must add one or more ESXi hosts and their respective physical NICs (PNICs) to the DVS where you deploy Cisco ACI Virtual Edge.

Note When you add hosts to a cluster on which Proactive HA is already configured, and then add the host or attach the host to a Cisco ACI Virtual Edge VMM domain, those hosts may not work properly in some circumstances. The hosts may not work properly in Proactive HA or when Cisco ACI Virtual Edge or OpFlex goes down. The hosts also may not go into quarantine mode although the health status of the host is correctly set to yellow in Cisco Cisco Application Policy Infrastructure Controller (APIC).

To fix the problem, disable Proactive HA on the cluster and then re-enable it.

Before you begin

- Create a VMM domain for Cisco ACI Virtual Edge. See the procedure Create a VMM Domain Profile for Cisco ACI Virtual Edge , on page 82 in this guide.
- Have at least one available PNIC on the host.

Procedure

Step 1 Log in to the VMware vSphere Client.

Step 2 From the **Home** page, go to **Networking** and then navigate to the Cisco ACI Virtual Edge DVS to which you want to add the hosts and PNICs.

Step 3 In the left navigation pane, right-click the host and choose **Add and Manage Hosts** from the drop-down list.

Alternatively, you can choose **Add and Manage Hosts** from the **ACTIONS** drop-down list at the top of the work pane.

Step 4 In the ***DVS*** **Add and Manage Hosts** dialog box, complete the following steps:

a) In the **Select Task** pane, click the **Add Hosts** radio button, and then click **NEXT**.

b) In the **Select Hosts** pane, click the green plus sign (+) next to **Add hosts**.

c) In the **Select New Hosts** dialog box, check the check box next to the host that you want to add and click **OK**.

You can choose multiple hosts.

d) In the **Manage Physical Adapters** pane, choose a PNIC for the host that you want to add and then click **Assign uplink**.

e) In the **Select an uplink** dialog box, choose an uplink for the adapter, and then click **OK**.

Repeat step 4d and 4e for each additional PNIC that you want to assign to an uplink from that host.

The **Manage Physical Adapters** pane shows that the PNIC has been assigned to the host.

f) Click **NEXT**.

g) In the **Manage VMkernel adapter** pane, view the configuration and then click **NEXT**.

h) In the **Migrate VM networking** pane, click **NEXT**.

i) In the **Ready to complete** pane, click **FINISH**.

Add ESXi Hosts and PNICs Using the Flash Version of the Cisco ACI vCenter Plug-in

Before you can install Cisco Application Centric Infrastructure (ACI) Virtual Edge, you must add one or more ESXi hosts and their respective PNICs to the new Cisco ACI Virtual Edge DVS.

Note When you add hosts to a cluster on which Proactive HA is already configured, and then add the host or attach the host to a Cisco ACI Virtual Edge VMM domain, those hosts may not work properly in some circumstances. The hosts may not work properly in Proactive HA or when Cisco ACI Virtual Edge or OpFlex goes down. The hosts also may not go into quarantine mode although the health status of the host is correctly set to yellow in Cisco Cisco Application Policy Infrastructure Controller (APIC).

To fix the problem, disable Proactive HA on the cluster and then re-enable it.

Before you begin

- Create a VMM domain for Cisco ACI Virtual Edge. See the procedure Create a VMM Domain Profile for Cisco ACI Virtual Edge , on page 82 in this guide.
- Have at least one available PNIC on the host.

Procedure

Step 1 Log in to the VMware vCenter Web Client.

Step 2 Go to **Networking**.

Step 3 In the left navigation pane, expand the Cisco ACI Virtual Edge folder and the folder for the newly created Cisco ACI Virtual Edge VMM domain.

Step 4 Right click the Cisco ACI Virtual Edge domain and choose **Add and Manage Hosts**.

Step 5 In the **Add and Manage Hosts** dialog box, in the **Select task** pane, click the **Add hosts** radio button and then click **Next**.

Step 6 In the **Select hosts** pane, click **New hosts**.

Step 7 In the **Select new hosts** dialog box, choose all the hosts that you want to add to the Cisco ACI Virtual Edge DVS, and then click **OK**.

Step 8 In the **Add and Manage Hosts** dialog box, click **Next**.

Step 9 Check the **Manage physical adapters** check box and then click **Next**.

Step 10 In the **Manage physical network adapters** pane, choose a PNIC, and click **Assign uplink**.

Step 11 In the **Select an Uplink** dialog box, choose an uplink for the adapter, and then click OK.

Step 12 Repeat Step 10 and Step 11 for each additional PNIC you want to add.

Step 13 Click **Next**, click **Next** again, and then click **Finish**.

Each host that you chose in Step 6 appears in the Cisco ACI Virtual Edge domain work pane.

What to do next

Upload the OVF file of the Cisco ACI Virtual Edge VM to the vCenter.

Cisco ACI Virtual Edge Installation Using the vCenter

After you fulfill the installation prerequisites, you can use the VMware vCenter to install Cisco Application Centric Infrastructure (ACI) Virtual Edge. You use the Cisco ACI plug-in for VMware vCenter, which automates the process.

There are two versions of the Cisco ACI plug-in for VMware vCenter. The original version—the Cisco ACI vCenter plug-in—is designed to work with Flash. However, Flash has been deprecated in the 6.7 version of VMware vSphere. Starting in version 6.7, Cisco ACI HTML5 vCenter plug-in, designed to work with HTML5, became available.

Procedures in this section note whether they can be performed with the Flash or HTML5 versions of the Cisco ACI plug-in for VMware vCenter.

You first upload the Cisco ACI Virtual Edge VM Open Virtualization Format (OVF) file to the vCenter content library. You can then deploy Cisco ACI Virtual Edge on the ESXi hosts.

Note

- If you use a local data store for content library storage, re-create the content library after you remove a host and then reattach it to vCenter. That is because the data store ID changes after the host is reattached, breaking the association between the content library and the data store.
- After you deploy Cisco ACI Virtual Edge, do not remove it from the vCenter inventory and add it back. Doing so removes all the configurations you made during deployment. Deploy a new Cisco ACI Virtual Edge instead of adding an existing one back to the inventory.

Uploading the Cisco ACI Virtual Edge VM OVF File to the VMware vCenter Content Library

Before you deploy the Cisco Application Centric Infrastructure (ACI) Virtual Edge on the ESXi hosts, you upload the Cisco ACI Virtual Edge virtual machine (VM) OVF file to the VMware vCenter. You can use one of two methods:

Upload the OVF File Using the HTML5 Version of the Cisco ACI vCenter Plug-in

You upload the Cisco Application Centric Infrastructure (ACI) Virtual Edge VM OVF file to the VMware vCenter using the HTML5 version of the Cisco ACI vCenter plug-in.

Before you begin

You must have done the following:

- Created a VMM domain for the Cisco ACI Virtual Edge on Cisco Application Policy Infrastructure Controller (APIC).
- Downloaded the folder with the OVF file to your computer.
- Made sure that the OVF file is compatible with the version of Cisco APIC.
- If you plan to use the Cisco ACI vCenter plug-in, ensure that the fabric has been successfully registered with the plug-in.

  See the chapter "Cisco ACI vCenter Plug-in" in the *Cisco ACI Virtualization Guide* for instructions for installing and using the plug-in.

Procedure

Step 1 Log in to the VMware vSphere Client.

Step 2 From the Menu drop-down list, choose **Content Libraries**.

You can use an existing content library or create one to receive the upload of the Cisco ACI Virtual Edge VM OVF. See VMware documentation for instructions for creating a content library.

Step 3 In the left navigation pane, right-click the library and choose **Import Item** from the drop-down list.

Step 4 In the **Import Library Item** dialog box, in the **Source file** area, complete one of the following steps:

- To upload the OVF file using a URL, click the **URL** radio button and enter the file URL.
- To upload the OVF file from a local file, click the **Local file** radio button, click **UPLOAD FILE**, and in the pop-up window, choose the file, and then click **Open**.

Step 5 In the **Destination** area, enter a name for the file in the **Item name** field.

Step 6 Click **IMPORT**.

Once the OVF file is uploaded to the content library, it appears in the content library work pane under the **Templates** tab.

Upload the OVF File Using the Flash Version of the Cisco ACI vCenter Plug-in

You upload the Cisco Application Centric Infrastructure (ACI) Virtual Edge VM OVF file to the vCenter using the Flash version of the Cisco ACI vCenter plug-in.

Before you begin

You must have done the following:

- Created a VMM domain for the Cisco ACI Virtual Edge on Cisco Application Policy Infrastructure Controller (APIC).
- Downloaded the folder with the OVF file to your computer.
- Made sure that the OVF file is compatible with the version of Cisco APIC.
- If you plan to use the Cisco ACI vCenter plug-in, ensure that the fabric has been successfully registered with the plug-in.

See the chapter "Cisco ACI vCenter Plug-in" in the *Cisco ACI Virtualization Guide* for instructions for installing and using the plug-in.

Procedure

Step 1 Log in to the vSphere Web Client.

Step 2 Choose **Content Libraries**.

You can use an existing content library or create one to receive the upload of the Cisco ACI Virtual Edge VM OVF. See VMware documentation for instructions for creating a content library.

Step 3 Choose the library and then click **Import item**.

Step 4 In the **Import library item** dialog box, click the **Browse** button.

Step 5 In the pop-up dialog box, choose the OVF file and click **Open**.

Another pop-up dialog box appears, which prompts you to choose the virtual machine disk (VMDK) file and XML file in the OVF folder.

Step 6 Choose the VMDK file and XML files and then click **OK**.

Once the OVF file is uploaded to the content library, it appears in the work pane under the **Templates** tab.

What to do next

Deploy Cisco ACI Virtual Edge on the ESXi hosts.

Deploy Cisco ACI Virtual Edge Using the HTML5 Version of the Cisco ACI vCenter Plug-in

After you upload the Cisco Application Centric Infrastructure (ACI) Virtual Edge VM OVF file to VMware vCenter, you deploy Cisco ACI Virtual Edge on the ESXi hosts.

Before you begin

You must have done the following:

- Created a VMM domain for the Cisco ACI Virtual Edge on Cisco APIC.
- Added one or more ESXi hosts and PNICs to the new Cisco ACI Virtual Edge DVS in VMware vCenter.
- Uploaded the Cisco ACI Virtual Edge VM OVF file to VMware vCenter.

Procedure

Step 1 Log in to the VMware vSphere Client.

Step 2 On the **Home** page, in the left navigation pane, click **Cisco ACI Fabric**.

Step 3 In the **Cisco ACI Fabric** navigation pane, choose the fabric from the **Fabric** drop-down list.

Step 4 In the left navigation pane, click **AVE** to display the list of domains associated with the fabric, and then double-click the domain where you want to deploy the Cisco ACI Virtual Edge VM.

Step 5 In the **AVE** work pane, click the **AVE** tab.

Step 6 (Optional) In the upper right of the work pane, click **Max concurrent tasks** pencil icon to choose the number of deployments to run at the same time.

If you want to deploy the Cisco ACI Virtual Edge VM on multiple hosts, if you specify the number of concurrent tasks, the VM will be deployed on the number of hosts that you specify. For example, if you choose to deploy the VM on five hosts and choose three tasks to run concurrently, deployment will proceed on three of the hosts at the same time while deployment for the other two hosts is queued.

Step 7 In the **Datacenter** table, check the check box for each host on which you want to deploy the Cisco ACI Virtual Edge VM.

Step 8 Click **DEPLOY AVE**.

Step 9 In the pop-up window, click **CONTINUE**.
The **New AVE Wizard** appears.

Step 10 In the **Version** pane, click the radio button for the Cisco ACI Virtual Edge version that you want to use and then click **NEXT**.

Step 11 In the **Networking** pane, click the radio button for the management port group that you want to use with the Cisco ACI Virtual Edge VM and then click **NEXT**.

Step 12 In the **Storage** pane, complete one of the following actions:

- Leave the check box checked for **Let vCenter select the Datastore Automatically** and then click **NEXT**.

  Uncheck the check box for **Let vCenter select the Datastore Automatically**, from the host drop-down list, choose a datastore, and then click **NEXT**.

Step 13 In the **Settings** pane, in the **Admin Password** and the **Confirm Admin Password** fields, enter your password for the VMware vCenter and then click **NEXT**.

Step 14 In the **Summary** pane, view information about the newly deployed VM and then click **FINISH**.

What to do next

Verify that the deployment is underway. In the **AVE** work pane, a **New AVE** pop-up window appears on the host where you deployed the VM. The host displays the percentage of how much of the deployment has completed. You also can click the clipboard icon at the upper right of the work pane and in the **ACI Tasks & Settings**, view information about the **New AVE** task.

Deploy Cisco ACI Virtual Edge Using the Flash Version of the Cisco ACI vCenter Plug-In

After you upload the Cisco ACI Virtual Edge VM OVF file to VMware vCenter, you deploy Cisco ACI Virtual Edge on the ESXi hosts. You can deploy Cisco ACI Virtual Edge as a component of a Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) in a remote site. Or you can deploy Cisco ACI Virtual Edge without making it part of a Cisco ACI vPod. See Cisco ACI vPod product documentation for more information.

Before you begin

You must have done the following:

- Created a VMM domain for the Cisco ACI Virtual Edge on Cisco APIC.
- Added one or more ESXi hosts and PNICs to the new Cisco ACI Virtual Edge DVS in VMware vCenter.
- Uploaded the Cisco ACI Virtual Edge VM OVF file to VMware vCenter.

Note If you use VMware vCenter 6.0 Web Client, the pop-up window for browsing to the OVF file may not appear. In that case, upload the OVF file, Virtual Machine Disk (VMDK) file, and XML file to the HTTP server. Then use the OVF file URL from the server to download the OVF file to the content library.

Procedure

Step 1 Log in to the vSphere Web Client.

Step 2 In the **Home** work pane, click the **Cisco ACI Fabric** icon.

Step 3 In the **Cisco ACI Fabric** navigation pane, click **ACI Virtual Edge**.

Step 4 In the **ACI Virtual Edge** work pane, if there are multiple virtual domains, choose the domain from the **Select an ACI Virtual Edge Domain** drop-down list; if there is only one virtual domain, skip to the next step.

Step 5 Choose the host or hosts on which you want to deploy Cisco ACI Virtual Edge.

Step 6 From the **ACI Virtual Edge version** drop-down list, choose the version to be deployed.

Step 7 From the **Management PortGroup** drop-down list, choose the management port group.

Step 8 From the **Datastore** drop-down list, choose **Custom**, click **Edit**.

Step 9 In the **Custom AVE Datastore selection** dialog box, choose a local or a remote data store for each Cisco ACI Virtual Edge.

Note To ensure a higher level of availability, we recommend that you choose a local data store if you have one.

Note You may not see all types of local storage in VMware vCenter. However, if you uncheck the **Use local datastore only** check box, VMware vCenter shows all local data stores. For details, see the document "When installing ESX/ESXi 4.x or 5.x to a physical server, the local SAS drive appears as a remote storage (1027819)" on the VMware website for details.

Step 10 In the **VM Admin Password** fields, enter a new password for the Cisco ACI Virtual Edge VMs.

Step 11 If you want to deploy the Cisco ACI Virtual Edge as part of a Cisco ACI vPod, complete the following steps:

a) Check the **vPod Mode** check box.

b) From the **vPod** drop-down list, choose the Cisco ACI vPod that you want to associate the Cisco ACI Virtual Edge with.

Step 12 Click **Install/Upgrade ACI Virtual Edge**.

Step 13 In the **Install** dialog box, click **Yes**.

In the work pane, the installed hosts display OpFlex status, the Cisco ACI Virtual Edge VM, and management IP. It could take a little while for OpFlex to come up.

What to do next

- Attach the correct EPGs to the VMM domain on the Cisco APIC controller or through VMware vCenter using the Cisco ACI vCenter plug-in.
- Put the VMs into the correct port groups in vCenter.

Cisco ACI Virtual Edge Installation Using the VMware PowerCLI

After you fulfill the preinstallation prerequisites, you can use the VMware PowerCLI to install Cisco ACI Virtual Edge.

You first set up the VMware Power CLI environment. You then download the .zip file containing the VMware PowerCLI file, import the Cisco ACI Virtual Edge module, then deploy the new Cisco ACI Virtual Edge VM from the vCenter content library.

Setting Up the PowerCLI Environment

Before you can use the PowerCLI to deploy the Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) or Cisco Application Centric Infrastructure (ACI) Virtual Edge virtual machines (VMs), you import the `CiscoAVE` PowerCLI module and establish a connection to the VMware vCenter.

Before you begin

Make sure that you have PowerCLI 6.0 Release 3 or later.

Procedure

Step 1 Download the `CiscoAVE` .zip file containing the high-level configuration files for Cisco ACI vPod or Cisco ACI Virtual Edge.

The zip file contains the following:

- `CiscoAVE.psm1`: The `CiscoAVE` VMware Power CLI module file
- `lib/`: The module library

Step 2 Import the `CiscoAVE` PowerCLI module using the **Import-Module** command.

Example:

```
PowerCLI C:\> Import-Module CiscoAVE.psm1
```

Step 3 Connect to the VMware vCenter using the standard PowerCLI commands: **Connect-VIServer** and **Connect-CisServer**.

The **Connect-CisServer** command is required for features such as tagging and managing the VMware vCenter content library.

Example:

```
PowerCLI C:\> Connect-VIServer -Server 172.23.143.235 -User admin -Password lab

Name    Port   User
----    ----   ----
172.23.143.235  443   admin
```

Example:

```
PowerCLI C:\> Connect-CisServer -Server 172.23.143.235 -User admin -Password lab

Name              User             Port
----              ----             ----
172.23.143.235    admin@localos    443
```

Managing the VMware vCenter Content Library Using the VMware PowerCLI

Upload the Open Virtualization Format (OVF) file to the VMware vCenter content library so the scripts in the file to deploy the virtual machines (VMs).

You can use an existing content library or create one. You create a new content library in the VMware vSphere Web Client UI or with the PowerCLI commands in this section.

Procedure

Step 1 Create a new VMware vCenter content library using the **New-LocalContentLibrary** command.

The following text shows the command syntax:

```
New-LocalContentLibrary [-Name] Object [-Datastore] Object [-Datacenter] Object
[CommonParameters]
```

Example:

```
PowerCLI C:\> New-LocalContentLibrary -Name ave-lib -Datastore 129-local -Datacenter mininet
Connecting to vCenter.....................................................[ok]
Creating content library 'ave-lib'........................................[ok]
```

Step 2 Upload an OVF file to the VMware vCenter content library using the **New-ContentLibraryItem** command.

The OVF (or .ova) file must be available on the local machine where you run the command.

The following text shows the command syntax:

```
New-ContentLibraryItem [-Name] Object [-ContentLibrary] Object [-Ovf] Object
[CommonParameters]
```

Example:

```
PowerCLI C:\> New-ContentLibraryItem -Name vpod-ova -ContentLibrary ave-lib -Ovf
L:\ova\aci-vpod.14.0.0.84.ova
Connecting to vCenter.....................................................[ok]
Extracting OVA............................................................[ok]
Validating................................................................[ok]
Uploading aci-vpod.14.0.0.84-disk1.vmdk...................................[ok]
Uploading aci-vpod.14.0.0.84.ovf..........................................[ok]
Finishing up..............................................................[ok]
```

Step 3 Remove an item from the VMware vCenter content library using the **Remove-LocalContentLibraryItem** command:

The following text shows the command syntax:

```
Remove-LocalContentLibraryItem [-Name] Object [-ContentLibrary] Object [CommonParameters]
```

Example:

```
PowerCLI C:\> Remove-LocalContentLibraryItem -Name vpod-14.0.0.84 -ContentLibrary vpod-ova
Connecting to vCenter.....................................................[ok]
Deleting content library item 'vpod-14.0.0.84'.......................[ok]
```

Deploying Cisco ACI Virtual Edge Using the VMware PowerCLI

If you have a Windows platform, you can use the VMware PowerCLI to install Cisco Application Centric Infrastructure (ACI) Virtual Edge. You can deploy Cisco ACI Virtual Edge as a component of a Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) in a remote site. Or you can deploy it without making it part of a Cisco ACI vPod. See Cisco ACI vPod documentation for more information.

Note You can use 'Get-Help' on any command to get help for any of the parameters. For example: **Get-Help New-LocalContentLibrary**

Procedure

Step 1 Take one of the following actions, depending on how you want to use Cisco ACI Virtual Edge:

Option	Description
If you want to deploy Cisco ACI Virtual Edge...	Then...
As part of a Cisco ACI vPod	Go to Step 2.
Not as part of a Cisco ACI vPod	Go to Step 3.

Step 2 Deploy Cisco ACI Virtual Edge as part of a Cisco ACI vPod using the **New-VPodAveVM** command.

The following text shows the command syntax:

```
New-VPodAveVM [-HostName] Object [-DomainName] Object [-MgmtPortgroupName] Object
[-AdminPassword] SecureString [-InfraVlan]
Object [-OvfItem] Object [-ApicVersion] Object [-VpodId] Object [[-Vtor1Ip] String]
[[-Vtor2Ip] String] [[-VtepIp]
String] [[-VtepNetmask] String] [[-VtepGateway] String] [[-Library] String] [[-DatastoreName]
 String] [[-Ip] String]
[[-Netmask] String] [[-Gateway] String] [[-Nameserver] String] [[-VmHostname] String]
[CommonParameters]
```

Example:

```
PowerCLI C:\> $pass = Read-Host -AsSecureString
********
PowerCLI C:\> New-VPodAveVM -HostName 198.51.100.15 -DomainName mininet -MgmtPortgroupName
 "VM Network"
-AdminPassword $pass -InfraVlan 4 -OvfItem cisco-ave-build312 -ApicVersion "4.0(1.0)" -VpodId
```

```
 2

Connecting to vCenter.....................................................[ok]
Validating configuration..................................................[ok]
Deploying OVF (this might take several minutes).....................[ok]
Applying Cluster configuration.....................................[ok]
Applying Cluster configuration.....................................[ok]
Applying VM configuration..........................................[ok]
Applying Host configuration........................................[ok]
Powering On VM.....................................................[ok]
```

Step 3 Deploy Cisco ACI Virtual Edge not as part of a Cisco ACI vPod using the **New-AveVM** command.

The following text shows the command syntax:

```
New-AveVM [-HostName] Object [-DomainName] Object [-MgmtPortgroupName] Object [-AdminPassword]
 SecureString [-InfraVlan]
<Object> [-OvfItem] Object [-ApicVersion] Object [[-Library] String] [[-DatastoreName]
String] [[-Ip] String] [[-Netmask]String] [[-Gateway] String] [[-Nameserver] String]
[[-VmHostname] String] [CommonParameter]
```

Example:

```
PowerCLI C:\> New-AveVM -HostName 198.51.100.15 -DomainName AVE-FI -MgmtPortgroupName
'VLAN418' -InfraVlan 5 -OvfItem "cisco-ave-2.0.0.466-r3" -Library 466 -Ip 10.197.143.195
-Netmask 255.255.255.0 -Gateway 198.51.100.160 -DatastoreName datastore-248 -ApicVersion
"4.0(1.0)" -Verbose

cmdlet New-AveVM at command pipeline position 1
Supply values for the following parameters:
AdminPassword: ********
Connecting to vCenter.....................................................[ok]
Validating configuration..................................................[ok]
Deploying OVF (this might take several minutes).....................[ok]
Applying Cluster configuration.....................................[ok]
Applying Cluster configuration.....................................[ok]
Applying VM configuration..........................................[ok]
Applying Host configuration........................................[ok]
Powering On VM.....................................................[ok]
PowerCLI C:\>
```

Step 4 Get a list of deployed Cisco ACI Virtual Edge virtual machines (VMs) using the **Get-AveVM** command.

The following text shows the command syntax:

```
Get-AveVM [<CommonParameters>]
```

Example:

```
PowerCLI C:\> Get-AveVM | Format-Table

VirtualMachine     HostName   DVS  ManagementIp
--------------     --------   ---  ------------
cisco-ave_198.51.100.15_mininet  198.51.100.15   mininet  198.51.100.41
```

Cisco ACI Virtual Edge Installation Using Python

After you fulfill the preinstallation prerequisites, you can use Python to install Cisco ACI Virtual Edge.

You first download the zip file containing the Python files, set up the environment to run Python, and then use Python commands to create a content library on vCenter, upload the Cisco ACI Virtual Edge VM OVF file to the vCenter content library, and then deploy the new VM from the content library.

Setting Up the Python Environment

Set up the Python environment so you can use Python to install Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) or Cisco Application Centric Infrastructure (ACI) Virtual Edge.

Note We strongly recommend that you use a virtual environment to avoid any Python dependency problems.

Before you begin

You must have done the following:

- Made sure that you have Python 2.7.9 or a later version.
- Made sure that you have VMware vCenter 6.0 GA U3 or later.
- Made sure that you have Git and PIP installed.

Procedure

Step 1 Download the .zip file containing the high-level Python configuration scripts for deploying Cisco ACI vPod and Cisco ACI Virtual Edge.

The .zip file contains the following:

- `get-avevm.py`: Gets the list of Cisco ACI Virtual Edge virtual machines (VMs) currently deployed.
- `new-avevm.py`: Deploy a new Cisco ACI Virtual Edge VM.
- `remove-avevm.py`: Removes a Cisco ACI Virtual Edge VM.
- `content-library.py`: Interact with the VMware vCenter content library.
- `get-vpodvm.py`: Get a list of Cisco ACI vPod VMs currently deployed.
- `new-vpodvm.py`: Deploy a new pair (one virtual spine [vSpine] and one virtual leaf [vLeaf]) of Cisco ACI vPod VMs.
- `remove-vpodvm.py`: Remove all Cisco ACI vPod VMs.
- `requirements.txt`: Python dependencies list used by the PIP package management system.

Step 2 (Optional but recommended) Set up a Python virtual environment.

a) Enter the following commands:

Example:

```
$ pip install virtualenv
$ virtualenv venv
```

b) Enter one of the following commands:

- If you have a Linux or Macintosh system, enter the following command:

```
$ . venv/bin/activate
```

- If you have a Windows system, enter the following command:

```
> ven\Scripts\activate
```

Step 3 Install the VMware vSphere Automation software development kit (SDK).

a) Download the VMware vSphere Automation SDK from GitHub; there is currently no up-to-date version in the Python Package Index (PyPi).

Example:

```
(venv) $ git clone https://github.com/vmware/vsphere-automation-sdk-python.git
(venv) $ cd vsphere-automation-sdk-python

Linux:

(venv) $ pip install --upgrade -r requirements.txt --extra-index-url file://`pwd`/lib

Windows:

> pip install --upgrade --force-reinstall -r requirements.txt --extra-index-url
file:///absolute_dir_to_sdk/lib
```

Step 4 Install all other dependencies.

Example:

```
(venv) $ cd ../
(venv) $ pip install -r requirements.txt
```

The `requirements.txt` file contains all the dependencies that the script relies on. Installing the dependencies in this file is a one-time task.

Managing the VMware vCenter Content Library Using Python

You upload the Open Virtualization Format (OVF) file to the VMware vCenter content library so the scripts in the file can deploy the virtual machines (VMs).

You can use an existing library or create a new one. You create a new content library in the VMware vSphere Web Client UI or with the Python commands in this section.

Procedure

Step 1 Create a new content library using the subcommand `Create`.

The following text shows the command usage:

```
usage: content-library.py [-h] --vcenter VCENTER --vc-username VC_USERNAME
[--vc-password VC_PASSWORD] [--silent] Create --name NAME --datacenter DATACENTER
--datastore DATASTORE
```

Example:

```
(venv) $ python content-library.py --vcenter 172.23.143.235 --vc-username admin --vcpassword
lab Create --name ave_repo --datacenter mininet --datastore 129-local
Connecting to vCenter.....................................................[ok]
Creating content library 'ave_repo'.....................................[ok]
```

Step 2 Copy the `ave vmdk` file to the datastore of any of the host in the VMware vCenter.

Example:

```
scp cisco-ave-2.1.1.321-disk1.vmdk root@10.23.238.203:/vmfs/volumes/datastore2/
```

Step 3 Upload the OVF file to the VMware vCenter content library using the subcommand **Upload**.

The OVF file must be available on the local machine where you run the Python script. Provide the full datastore path of the copied `vmdk` file in `–vmdk-ds-path`.

The following text shows the command usage:

```
usage: content-library.py [-h] --vcenter VCENTER --vc-username VC_USERNAME
[--vc-password VC_PASSWORD] [--silent] Upload --library LIBRARY --item ITEM --path PATH
[--vmdk-ds-path VMDK_DS_PATH]
```

Example:

```
(venv) $ python content-library.py --vcHost 10.23.219.150 --vcUser 'administrator' --vcPwd
 'lab' Upload --library repo --item cisco-ave-2.1.1.321.ovf --path
/Users/User/dev/ovf/cisco-ave-2.1.1.321.ovf --vmdk-ds-path
ds:///vmfs/volumes/59348426-b1a50255-8787-cc167ee18b76/cisco-ave-2.1.1.321-disk1.vmdk
Connecting to vCenter.....................................................[ok]
Extracting OVA............................................................[ok]
Validating................................................................[ok]
Uploading aci-vpod.14.0.0.84-disk1.vmdk...................................[ok]
Uploading aci-vpod.14.0.0.84.ovf..........................................[ok]
Finishing up..............................................................[ok]
```

Step 4 Remove an item from the content library using the subcommand **Remove**.

The following text shows the command usage:

```
usage: content-library.py [-h] --vcenter VCENTER --vc-username VC_USERNAME
[--vc-password VC_PASSWORD] [--silent] Remove --library LIBRARY --item ITEM
```

Example:

```
(venv) $ python content-library.py --vcenter 172.23.143.235 --vc-username admin --vcpassword
lab Remove --library repo --item vpod-14.0.0.84
Connecting to vCenter.....................................................[ok]
Deleting content library item 'vpod-14.0.0.84'.....................[ok]
```

Deploying Cisco ACI Virtual Edge Using Python

You can use a Python script to deploy Cisco Application Centric Infrastructure (ACI) Virtual Edge. You can deploy Cisco ACI Virtual Edge as a component of a Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod) in a remote site. Or you can deploy it without making it part of a Cisco ACI vPod. See Cisco ACI vPod documentation for more information.

Note You can enter `-h` on any script to get help for any of the parameters. Example:

```
# python new-avevm.py -h
```

Before you begin

- Make sure that you have set up the Python environment. See the procedure Setting Up the Python Environment, on page 32 in this guide.
- If you used a proxy to access the Internet when setting up the Python environment, unset it before running Python scripts:

```
unset http_proxy
unset https_proxy
```

Procedure

Step 1 Take one of the following actions, depending on how you want to use Cisco ACI Virtual Edge:

Option	Description
If you want to deploy Cisco ACI Virtual Edge...	Then...
as part of a Cisco ACI vPod	Go to Step 2.
not as part of a Cisco ACI vPod	Go to Step 3.

Step 2 Deploy Cisco ACI Virtual Edge as part of a Cisco ACI vPod using the `vPod` subcommand.

The following text shows the command usage:

```
usage: new-avevm.py [-h] [--silent] --vcenter VCENTER --vc-username
VC_USERNAME [--vc-password VC_PASSWORD] --host-name
HOST_NAME --domain-name DOMAIN_NAME --mgmt-pg MGMT_PG
[--admin-password ADMIN_PASSWORD] --infra-vlan INFRA_VLAN
--ovf-item OVF_ITEM [--library LIBRARY]
[--datastore DATASTORE] [--ip IP] [--netmask NETMASK]
[--gateway GATEWAY] [--nameserver NAMESERVER]
[--vm-hostname VM_HOSTNAME] --apic-version APIC_VERSION
vPod --vpod-id VPOD_ID [--vtor1-ip VTOR1_IP]
[--vtor2-ip VTOR2_IP] [--vtep-ip VTEP_IP]
[--vtep-netmask VTEP_NETMASK]
[--vtep-gateway VTEP_GATEWAY]
```

Example:

```
python new-avevm.py --vcenter 172.23.143.235 --vc-username 'administrator@vsphere.local'
--vc-password 'vcpassword' --host-name 172.23.143.129 --domain-name 'ave-dom1' --mgmt-pg
'VM Network' --infra-vlan 10 --ovf-item cisco-ave-2.0.0.476 --admin-password 'adminpassword'
 --apic-version '4.0(0.0)' vPod --vpod-id 2

Connecting to vCenter.....................................................[ok]
Validating configuration..................................................[ok]
Deploying OVF (this might take several minutes)...........................[ok]
Applying Cluster configuration............................................[ok]
Applying Cluster configuration............................................[ok]
Applying VM configuration.................................................[ok]
Applying Host configuration...............................................[ok]
Powering On VM............................................................[ok]
```

Note If the management port group is on a VMware VDS, you must specify the VDS name in the following format: `--mgmt-pg 'vds-name/portgroup-name'`

Note To use a static management IP address, use the `--ip` parameter, placed before the `vPod` subcommand:

```
[...] --ip 172.31.100.11 --netmask 255.255.255.0 --gateway 172.31.100.1 --nameserver
 172.23.140.25 vPod [...]
```

Step 3 Deploy Cisco ACI Virtual Edge not as part of a Cisco ACI vPod using the **Enterprise** subcommand.

The following text shows the command usage:

```
usage: new-avevm.py [-h] [--silent] --vcenter VCENTER --vc-username
VC_USERNAME [--vc-password VC_PASSWORD] --host-name
HOST_NAME --domain-name DOMAIN_NAME --mgmt-pg MGMT_PG
[--admin-password ADMIN_PASSWORD] --infra-vlan INFRA_VLAN
--ovf-item OVF_ITEM [--library LIBRARY]
[--datastore DATASTORE] [--ip IP] [--netmask NETMASK]
[--gateway GATEWAY] [--nameserver NAMESERVER]
[--vm-hostname VM_HOSTNAME] --apic-version APIC_VERSION
{vPod,Enterprise} ...
```

Example:

```
(venv) $ python new-avevm.py --vcenter 172.23.143.235 --vc-username admin --vc-password
lab --host-name 172.23.143.129 --domain-name mininet --mgmt-pg 'VM Network' --infra-vlan 4

--ovf-item cisco-ave-build312 --apic-version '4.0(0.0)' --admin-password password Enterprise

Connecting to vCenter.....................................................[ok]
Validating configuration..................................................[ok]
Deploying OVF (this might take several minutes).....................[ok]
Applying Cluster configuration.....................................[ok]
Applying Cluster configuration.....................................[ok]
Applying VM configuration..........................................[ok]
Applying Host configuration........................................[ok]
Powering On VM.....................................................[ok]
```

Step 4 Get a list of deployed Cisco ACI Virtual Edge virtual machines (VMs) using the `get-avevm.py` script.

The following text shows the script usage:

```
usage: get-avevm.py [-h] [--silent] --vcenter VCENTER --vc-username
VC_USERNAME [--vc-password VC_PASSWORD]
```

Example:

```
(venv) $ python get-avevm.py --vcenter 172.23.143.235 --vc-username admin --vc-password lab

+----------------------------------+----------------+---------+----------------+
| Virtual Machine | Host | Domain | Management IP |
+----------------------------------+----------------+---------+----------------+
| cisco-ave_172.23.143.129_mininet | 172.23.143.129 | mininet | 172.31.143.146 |
| cisco-ave_172.23.143.228_mininet | 172.23.143.228 | mininet | None |
+----------------------------------+----------------+---------+----------------+
```

Verify the Cisco ACI Virtual Edge Deployment

After you deploy Cisco Application Centric Infrastructure (ACI) Virtual Edge, verify the deployment by ensuring that the interface that is used to communicate with Cisco ACI Virtual Edge (kni0) has a virtual tunnel endpoint (VTEP) IP address. Also verify that OpFlex is up.

Before you begin

You must have deployed Cisco ACI Virtual Edge in VMware vCenter.

Procedure

Step 1 Enter the **ipconfig** command and examine the output.

Example:

```
kni0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.9.3  netmask 255.255.252.0  broadcast 192.168.11.255
        inet6 fe80::250:56ff:fea7:fac  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:a7:0f:ac  txqueuelen 1000  (Ethernet)
        RX packets 374443  bytes 52541802 (50.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 161054  bytes 20000611 (19.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 2 Check if OpFlex is up by entering the appropriate **vemcmd** command:

- If you are using Cisco ACI Virtual Edge as part of Cisco ACI Virtual Pod (vPod), enter the command **vemcmd show opflex cloud**, as shown in the following example:

```
AVE-36:~$ vemcmd show opflex cloud
Status: READY
Peer 1, host: 192.168.8.16, port: 8009, status: READY
Peer 2, host: 192.168.8.17, port: 8009, status: READY
Dvs name: comp/prov-VMware/ctrlr-[vpod]-vc/sw-dvs-1983
```

- If you are using Cisco ACI Virtual Edge and it is *not* part of Cisco ACI vPod, enter the command **vemcmd show opflex**, as shown in the following example:

```
cisco-ave:~$ vemcmd show opflex
Status: 12 (Active)
Channel0: 12 (Active), Channel1: 12 (Active)
Dvs name: comp/prov-VMware/ctrlr-[vpod]-vc/sw-dvs-1983
Remote IP: 10.0.0.30 Port: 8000
Infra vlan: 4093
FTEP IP: 10.0.0.32
Switching Mode: LS
Encap Type: VXLAN
NS GIPO: 228.1.1.1
```

What to do next

Read the sections View Cisco ACI Virtual Edge Licenses Using the GUI, on page 37 and Post-Installation Configuration, on page 40 in this guide.

View Cisco ACI Virtual Edge Licenses Using the GUI

Beginning with Cisco APIC Release 3.2(1), you can view Cisco ACI Virtual Edge licenses in the Cisco ACI Fabric as part of the Smart Licensing feature.

You also can use NX-OS style CLI commands to view licensing information. For detailed information, see the knowledgebase article *Smart Licensing* on Cisco.com.

Before you begin

You must register for Smart Licensing. See the knowledgebase article *Smart Licensing* on Cisco.com.

Procedure

Step 1 Log in to Cisco APIC.

Step 2 Go to **System** > **Smart Licensing**.
The central pane, in the **Smart License Usage** area, displays a list of licenses, their number, and status. For the Cisco ACI Virtual Edge license, the **Count** column displays the number of Cisco ACI Virtual Edge instances in the Cisco ACI Fabric. Only Cisco ACI Virtual Edge instances that are turned on and connected through OpFlex are counted.

The **Count** column displays the number of Cisco ACI Virtual Edge instances present in the VMware vCenter DVS that is managed by Cisco APIC. Even Cisco ACI Virtual Edge instances that are not powered on are counted for licensing.

Note Cisco ACI Virtual Edge license count may be incorrect while upgrade or downgrade is being performed.

Configuring a Static IP Address in VMware vCenter

After you deploy Cisco Application Centric Infrastructure (ACI) Virtual Edge, you can configure a static IP address for it in VMware vCenter. You perform the procedure after accessing VMware vCenter using either the Cisco ACI HTML5 vCenter plug-in or the Flash version of the Cisco ACI vCenter plug-in:

- Configure a Static IP Address Using the HTML5 Version of the VMware vSphere Client, on page 38
- Configuring a Static IP Address in VMware vCenter, on page 39

Configure a Static IP Address Using the HTML5 Version of the VMware vSphere Client

You can configure a static IP address for the Cisco Application Centric Infrastructure (ACI) Virtual Edge. If you do not use Python or the VMware PowerCLI, you can configure the static IP address in the VMware vCenter. Complete this procedure if you use the HTML5 version of the Cisco ACI HTML5 vCenter plug-in.

Before you begin

You must have installed Cisco ACI Virtual Edge in the VMware vCenter.

Procedure

Step 1 Log in to the VMware vSphere Client.

Step 2 Go to **Hosts and Clusters** > **Datacenter** > ***host*** and select the Cisco ACI Virtual Edge virtual machine (VM) on the host.

Step 3 In the menu bar, click the square red icon to shut down the the Cisco ACI Virtual Edge VM, and then in the **Confirm Power Off** dialog box, click **YES**.

Step 4 With the Cisco ACI Virtual Edge VM chosen in the left navigation pane, click **Configure** and then click **vApp Options**.

Step 5 Click **EDIT** in the upper right of the work pane.

Step 6 In the **Edit vApp Options** dialog box, complete the following steps:

a) Ensure that the **IP Allocation** tab is chosen.
b) In the **Authoring** area, leave the **IP allocation** check boxes checked for **DHCP** and **OVF environment**.
c) In the **Deployment** area, choose **Static - Manual** from the **IP allocation** drop-down list.
d) Click **OK**.

Step 7 Enter the IP address, mask, and subnet information for unrecognized OVF by completing the following steps:

a) In the **vApp Options** work pane, click the **Configure** tab.
b) In the **Properties** area at the bottom of the work pane, click the radio button for the **Management Address**, and then click **Set Value**.
c) In the **Set Value** dialog box, in the **IP value** field, enter the IP management address, and then click **OK**.
d) Repeat step 7b and 7c for the **Management Netmask** and **Management Gateway**.

Step 8 In the left navigation pane, right-click the Cisco ACI Virtual Edge VM, and choose **Power** from the drop-down list. then choose **Power On**.

Configuring a Static IP Address in VMware vCenter

You can configure a static IP address for the Cisco Application Centric Infrastructure (ACI) Virtual Edge. If you do not use Python or the VMware PowerCLI, you can configure the static IP address in the VMware vCenter.

Procedure

Step 1 Log in to the VMware vCenter Web Client.

Step 2 Power off the Cisco ACI Virtual Edge.

Step 3 Navigate to the host and virtual machine (VM) and then choose the **Configure** tab.

Step 4 In the VM pane, choose **Edit** and then in the **Edit Settings** dialog box, choose **vApp Options**.

Step 5 In the **Deployment** area, from the **IP allocation** drop-down list, choose **Static - Manual**.

Step 6 In the **Unrecognized OVF sections** area, enter the IP address, mask and gateway information.

Step 7 Click **OK**.

Post-Installation Configuration

After you install the Cisco ACI Virtual Edge, perform key configuration tasks:

- Deploy an application profile, which includes creating a tenant, application profile, EPGs, filters, and contracts, and assigning port groups to VMs. Then verify the application profile.

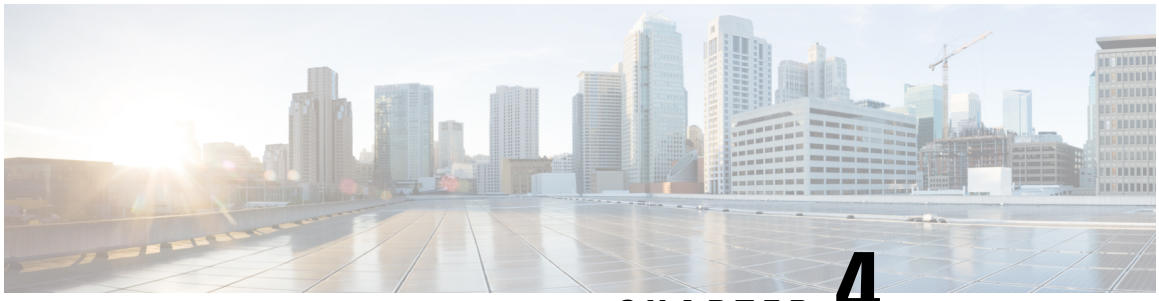
  See the Cisco APIC Basic Configuration Guide for instructions.

- If you want to use Distributed Firewall, Enable it after installation. See the chapter "Distributed Firewall" in the Cisco ACI Virtual Edge Configuration Guide for instructions.

- In order for Cisco ACI Virtual Edge to forward multi-destination traffic—especially when traffic goes through a blade switch—configure an IGMP querier under the infra BD subnet. This enables devices to build their Layer 2 multicast tree.

  See the section "Configuring IGMP Querier and Snooping" in the Cisco ACI Virtual Edge Configuration Guide for instructions.

You can find instructions for other configuration tasks—including microsegmentation, SPAN, intra-EPG isolation enforcement, mixed-mode encapsulation, and BPDU features—in the Cisco ACI Virtual Edge Configuration Guide.



CHAPTER 4

Migration from Cisco AVS to Cisco ACI Virtual Edge

This chapter describes migration from Cisco AVS to Cisco ACI Virtual Edge, including different methods.

About Migration from Cisco AVS to Cisco ACI Virtual Edge

If you use Cisco AVS, you can migrate hosts and their VMs from that switch to Cisco ACI Virtual Edge.

After fulfilling several prerequisites, you use vCenter plug-in to use one of three methods to migrate from Cisco Application Virtual Switch (AVS) to Cisco ACI Virtual Edge.

Note Beginning with Cisco Application Policy Infrastructure Controller (APIC) Release 5.0(1), Cisco AVS is no longer supported. If you want to migrate from Cisco AVS to Cisco ACI Virtual Edge, do so before you upgrade to Cisco APIC 5.0(1).

Methods of Migrating from Cisco AVS to Cisco ACI Virtual Edge

You can use one of three methods in the vCenter plug-in to migrate from Cisco AVS to Cisco ACI Virtual Edge. Each method automates the migration through the same vCenter GUI screens. The method you choose depends on your setup and network topology:

- **DRS**—All the hosts to be migrated are in the same Distributed Resource Scheduler (DRS) cluster. When the vCenter plug-in puts a host into maintenance mode, DRS automatically migrates the host's VMs to another host in the cluster.

  With this method, any active VMs present on the host are automatically moved out of the host, resulting in minimal traffic loss.

- **Reserve Host**—You choose a reserve host, and the vCenter plug-in migrates all active VMs to this host before proceeding with the migration.

  With this method, any active VMs present on the host are automatically moved out of the host, resulting in minimal traffic loss.

- **In-Place Migration**—The host is migrated to Cisco ACI Virtual Edge with active VMs running on the host. You may want to use this method if don't want to move VMs to another host and want only to deploy Cisco ACI Virtual Edge.

Note This method causes significant outage to the VMs' network connectivity.

DRS Migration Workflow

The following is for migrating when there are no hosts in the cluster with Cisco ACI Virtual Edge running with OpFlex online.

1. The host is put into maintenance mode.
2. The Cisco ACI Virtual Edge DVS is added to the host.

   Make sure that the Cisco ACI Virtual Edge DVS has inside/outside and intra port groups and the same port groups that are on the Cisco AVS.
3. The PNICs and vmknic are moved from the Cisco AVS DVS to the Cisco ACI Virtual Edge DVS.
4. The port group of powered-off VMs on the host is updated from Cisco AVS to Cisco ACI Virtual Edge.
5. The Cisco AVS DVS is removed from the host.
6. The Cisco AVS module is uninstalled from the host (if you chose to uninstall it).
7. An affinity rule is placed on the DRS cluster.

   The affinity rule prevents DRS from moving any VMs running on the Cisco ACI Virtual Edge DVS to the host being upgraded until the Cisco ACI Virtual Edge VM is fully deployed.
8. The host is taken out of maintenance mode.
9. The Cisco ACI Virtual Edge VM is deployed on the host.
10. The OpFlex agent comes online.
11. The affinity rule on the DRS cluster is removed.

    The host has now finished migrating from Cisco AVS to Cisco ACI Virtual Edge.

When you migrate another host in the cluster, the DRS cluster checks if any hosts in the cluster are running Cisco ACI Virtual Edge. When it finds one, it moves VMs from the second host to the host running Cisco ACI Virtual Edge through a cross-DVS VMotion. VMs are left on their original host if the new host does not have sufficient resources. When multiple hosts run Cisco ACI Virtual Edge, the DRS cluster balances the load among them during migration.

Reserve Host Migration Workflow

If the reserve host is running Cisco AVS, then the active VMs are moved to the reserve host using standard VMotion. If the reserve host is running Cisco ACI Virtual Edge, the active VMs are moved to the reserve host using cross-DVS VMotion.

Note If you are using the reserve host migration method, and the reserve host is running Cisco ACI Virtual Edge, all hosts must run ESXi version 6.0. Otherwise, cross-DVS VMotion does not work.

1. The host is put into maintenance mode.
2. The Cisco ACI Virtual Edge DVS is added to the host.
3. The PNICs and vmknic are moved from the Cisco AVS DVS to the Cisco ACI Virtual Edge DVS.
4. The port group of powered-off VMs on the host is updated from Cisco AVS to Cisco ACI Virtual Edge.
5. The Cisco AVS DVS is removed from the host.
6. The Cisco AVS module is uninstalled from the host.
7. An affinity rule is placed on the DRS cluster. This prevents any VMs running on the Cisco ACI Virtual Edge DVS to move to the host being upgraded.
8. The host is taken out of maintenance mode.
9. The Cisco ACI Virtual Edge VM is deployed on the host.
10. The OpFlex Agent comes online.
11. The VMs that were automatically moved by VMotion to the reserve host in Step 1 are moved by VMotion back to the host that you just migrated to Cisco ACI Virtual Edge.

    If VMs were moved to the reserve host using standard VMotion, then cross-DVS VMotion is used to move them back. If VMs were moved to the reserve host using cross-DVS VMotion, then standard VMotion is used to move them back.

In-Place Migration Workflow

1. The Cisco ACI Virtual Edge DVS is added to the host.
2. The Cisco ACI Virtual Edge VM is deployed on the host.

   No uplinks are connected, and OpFlex is down.
3. The PNICs and vmknic are moved from the Cisco AVS DVS to the Cisco ACI Virtual Edge DVS.

   The VMs running on Cisco AVS lose network connectivity at this point.
4. The OpFlex Agent comes online.
5. The VM port groups are updated from Cisco AVS to Cisco ACI Virtual Edge.
6. The Cisco AVS DVS is removed from the host.

Note The Cisco ACI Virtual Edge module remains installed on the host using this method; uninstalling it requires putting the host into maintenance mode.

Prerequisites for Migrating from Cisco AVS to Cisco ACI Virtual Edge

Before you can migrate hosts and VMs from Cisco Application Virtual Switch (AVS) to Cisco Application Centric Infrastructure (ACI) Virtual Edge, perform the following tasks:

- Create a VMM domain for Cisco ACI Virtual Edge in Cisco APIC.

  The associated DVS with all port groups already must be created in vCenter.

- Disable ARP Learning on the Cisco AVS VMM domain before beginning the migration.

  Cisco ACI Virtual EdgeVMM domain creation will fail if ARP Learning is enabled on the Cisco AVS VMM domain.

- Make sure that OpFlex is online so the hosts can migrate.

- Upload the Cisco ACI Virtual Edge OVF file to the vCenter content library.

  See the procedure Upload the OVF File Using the Flash Version of the Cisco ACI vCenter Plug-in , on page 24 in this guide for instructions.

- Make sure that all VMs on the hosts that you plan to upgrade are using shared storage.

- Make sure that any EPGs used by vmknics use native mode switching.

  Note Unless they are backed by EPGs, vmknics will not be migrated.

- In order to use the Cisco ACI Virtual Edge management tools (including the ACI vCenter plug-in), we recommend that you use vCenter 6.0 Update 3 or later.

- Make sure that all hosts run ESXi 6.0 or later. Cross-DVS VMotion fails unless all hosts being migrated—and the reserve host when using reserve-host migration—run earlier versions of ESXi.

- Make sure that the Enhanced VMotion Compatibility (EVC) mode for the DRS cluster is set to Nehalem or higher.

- Plan VMotion migration to not exceed the limit on Cisco ACI Virtual Edge installed hosts; the limit is 300 VMs per ESXi host.

- If Cisco ACI Virtual Edge will be deployed in mixed-mode or VLAN mode, create two VLAN pools: one for primary encapsulation and one for private VLAN implementation.

  The role for the private VLAN pool must be internal. If Cisco ACI Virtual Edge will be deployed in VXLAN mode, only a private VLAN pool is necessary.

Note Alternatively, if you migrate from Cisco AVS to Cisco ACI Virtual Edge using the Cisco APIC GUI, you can create the private VLAN pools during migration.

Migrate the Cisco AVS VMM Domain to Cisco ACI Virtual Edge Using the GUI

You can use the Cisco APIC GUI to migrate an existing Cisco AVS VMM domain to a new Cisco ACI Virtual Edge domain. This method is easier than creating a new VMM domain, which requires that you manually reproduce most of the configuration of the Cisco AVS domain.

All the properties of the original domain remain; however, you must re-enter your vCenter credentials. The original VMM domain remains.

Note You can migrate only one Cisco AVS VMM domain at a time.

Note All EPGs associated to the original VMM domain are copied to the new Cisco ACI Virtual Edge VMM domain with Cisco ACI Virtual Edge switching mode.

Before you begin

Create a Cisco AVS domain. See the procedure Create vCenter Domain, Interface, and Switch Profiles Using the GUI, on page 15 in this guide.

Procedure

Step 1 Log in to the Cisco APIC.

Step 2 Go to **Virtual Networking** > **Inventory**.

Step 3 In **Inventory** navigation pane, expand the **VMM Domains** and the **VMware** folders, right-click the Cisco AVS domain that you want to migrate, and then choose **Migrate to Cisco AVE**.

Step 4 In the **Migrate To Cisco AVE** dialog box, complete the following actions:

a) In the **Virtual Switch Name** field, enter a name for the new Cisco ACI Virtual Edge VMM domain.

b) From the **VLAN Pool** drop-down list, choose or create a VLAN pool.

If Cisco ACI Virtual Edge will be deployed in mixed mode or VLAN mode, create two VLAN pools: one for primary encapsulation and one for private VLAN implementation. The role for the private VLAN pool must be internal. If Cisco ACI Virtual Edge will be deployed in VXLAN mode, only a private VLAN pool is necessary.

c) In the **vCenter Credentials** area, double-click **Re-enter required** and enter and confirm your vCenter password.

d) Click **Update** and then click **OK**.

What to do next

Follow instructions in the section Migrate from Cisco AVS to Cisco ACI Virtual Edge Using the Cisco ACI vCenter Plug-in, on page 46 in this guide.

Migrate from Cisco AVS to Cisco ACI Virtual Edge Using the Cisco ACI vCenter Plug-in

You use the Cisco ACI vCenter plug-in to migrate hosts and their VMs from Cisco AVS to Cisco ACI Virtual Edge, choosing one of three migration methods. The procedure is virtually the same for each method.

Before you begin

You must have fulfilled the tasks in the section Prerequisites for Migrating from Cisco AVS to Cisco ACI Virtual Edge , on page 44 in this guide. You also must have migrated the VMM domain; see the section Migrate the Cisco AVS VMM Domain to Cisco ACI Virtual Edge Using REST API, on page 99 or the section Migrate the Cisco AVS VMM Domain to Cisco ACI Virtual Edge Using the GUI, on page 45 in this guide.

Procedure

Step 1 Log in to the vSphere Web Client.

Step 2 In the **Home** work pane, click the **Cisco ACI Fabric** icon.

Step 3 In the **Cisco ACI Fabric** navigation pane, click **Infrastructure**.

Step 4 Click the **AVS** tab at the top of the page.

Step 5 Click the **Refresh ACI Domains** button.

Step 6 In the **Cisco AVS** work pane, from the **Select an AVS Domain** drop-down list, choose a kernel Cisco AVS domain.

Step 7 On the right side of the **Cisco AVS** work pane, check the appropriate check box to choose each host that you want to migrate.

Step 8 Click **Migrate to ACI Virtual Edge.**.
The **AVS Migration** dialog box appears.

Step 9 From the **Mode** drop-down list, choose a migration method.

You can choose **DRS**, **Reserve Host**, or **In-Place**. See the section Methods of Migrating from Cisco AVS to Cisco ACI Virtual Edge, on page 41 in this guide for details.

You can choose to retain the Cisco AVS kernel module by checking the retention check box.

Step 10 If you chose **Reserve Host** in the previous step, choose the host from the **Reserve Host** drop-down list that appears.

Step 11 From the **Target VDS** area, choose the Cisco ACI Virtual Edge domain that you want to migrate the host or hosts to.

If you have more than one Cisco ACI Virtual Edge domain, you choose the domain from a drop-down list.

Step 12 From the **ACI Virtual Edge** drop-down list, choose the Cisco ACI Virtual Edge installation configuration.

Step 13 From the **Management** drop-down list, choose the management port group for the management interface of the Cisco ACI Virtual Edge VM.

Step 14 From the **Datastore** drop-down list, choose **Custom**, click **Edit**.

Step 15 In the **Custom AVE Datastore selection** dialog box, choose a local or a remote data store for each Cisco ACI Virtual Edge.

Note To ensure a higher level of availability, we recommend that you choose a local data store if you have one.

Note You may not see all types of local storage in vCenter. However, if you uncheck the **Use local datastore only** check box, vCenter shows all local data stores. For details, see the document "When installing ESX/ESXi 4.x or 5.x to a physical server, the local SAS drive appears as a remote storage (1027819)" on the VMware website for details.

Step 16 In the **VM Password** fields, enter the admin password for the Cisco ACI Virtual Edge VM.

Step 17 Make sure that in the **Migration Validity** area, you see the message "The configuration is valid," and then click **OK**.

If the configuration is not valid, you see an error message indicating which preflight check failed and giving the reason that the migration cannot proceed. Fix the issue that caused the validation and try the migration again.

CHAPTER 5

Migration from VMware VDS to Cisco ACI Virtual Edge

This chapter describes migration from VMware VDS to Cisco ACI Virtual Edge, including different methods.

About Migrating a VDS Domain to Cisco ACI Virtual Edge

If you have VMware VDS domains configured, you can migrate that domain to Cisco ACI Virtual Edge. The migration enables you to take advantage of Cisco ACI Virtual Edge features. These include the ability to use VXLAN encapsulation and Distributed Firewall.

When you migrate a VDS domain, Cisco APIC creates inside and outside and port groups on the DVS in vCenter. The domain appears as a Cisco ACI Virtual Edge domain. However, you can choose to have some endpoints operate in **native** VDS mode and other operate in **AVE** (Cisco ACI Virtual Edge) mode. That is, endpoints are switched through the VDS or the Cisco ACI Virtual Edge.

You can migrate VMware VDS domains to Cisco ACI Virtual Edge by using the Cisco APIC GUI, the NX-OS style CLI, or REST API.

Note Changing the switching mode from **native** to **AVE** (Cisco ACI Virtual Edge) on an EPG requires changing the underlying switching platform from regular VMware DVS to Cisco ACI Virtual Edge. It also requires moving all the associated ports from DVS to Cisco ACI Virtual Edge.

This operation requires reprogramming of the port group associated with that EPG. That in turn requires a vCenter operation. It make take a few seconds for this operation to complete and for ports to show up in forwarding state on the Cisco ACI Virtual Edge switching platform. It length of time depends on the vCenter load as well as the number of endpoints that reside on the EPG that is being moved from **native** to **AVE** mode.

Migrate a VDS Domain to Cisco ACI Virtual Edge Using the GUI

This procedure migrates the existing VMM domain to a new Cisco ACI Virtual Edge VMM domain. The properties of the original VMM domain are preserved. However, no copy of the original VMM domain remains.

Before you begin

- You have created a VDS domain. See the procedure "Creating a VMM Domain Profile" in the *Cisco ACI Virtualization Guide*.
- If Cisco ACI Virtual Edge will be deployed in mixed-mode or VLAN mode, create two VLAN pools: one for primary encapsulation and one for private VLAN implementation.

  The role for the private VLAN pool must be internal. If Cisco ACI Virtual Edge will be deployed in VXLAN mode, only a private VLAN pool is necessary.

  Note Alternatively, you can create the private VLAN pool when you migrate from VDS to Cisco ACI Virtual Edge.

- You have disabled First-Hop Security.

  Take the following steps:

  1. Under the **Tenants** tab, select your tenant, navigate to the bridge domain on which First Hop Security is enabled. Click the **Advanced/Troubleshooting** tab, and in the work pane, delete the policy.
  2. Under the **Tenants** tab, navigate to the EPG on which the trust control policy is applied, click the **General** tab, and in the work pane, remove the FHS trust control policy.

Procedure

Step 1 Log in to the Cisco APIC.

Step 2 Go to **Virtual Networking** > **Inventory**.

Step 3 In the **Inventory** navigation pane, expand the **VMM Domains** folder and the **VMware** folder, right-click the VDS domain that you want to migrate, and then choose **Migrate to Cisco AVE**.

Step 4 In the **Migrate To Cisco AVE** dialog box, complete the following actions:

a) In the **AVE Fabric-Wide Multicast Address** field, enter a multicast address.

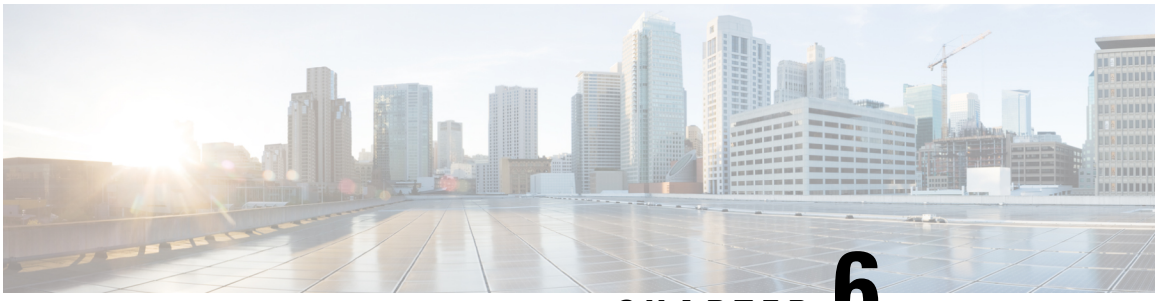
b) From the **Pool of Multicast Addresses (one per-EPG)** drop-down list, choose or create a pool.

c) From the VLAN Pool drop-down list, choose or create a VLAN pool.

If Cisco ACI Virtual Edge will be deployed in mixed-mode or VLAN mode, create two VLAN pools: one for primary encapsulation and one for private VLAN implementation. The role for the private VLAN pool must be internal. If Cisco ACI Virtual Edge will be deployed in VXLAN mode, only a private VLAN pool is necessary.

d) Click **OK**.

The domain that you migrated retains its original name. However, if you click the domain in the navigation pane, you can see that the value for **Virtual Switch** changed from **Distributed Switch** to **Cisco AVE**.



CHAPTER 6

Cisco ACI Virtual Edge Upgrade

This chapter describes upgrading the Cisco ACI Virtual Edge, including prerequisites and instructions.

About Cisco ACI Virtual Edge Upgrades

Upgrading Cisco Application Centric Infrastructure (ACI) Virtual Edge is similar to installing it. You download a new Cisco ACI Virtual Edge OVF file from Cisco.com and upload it to the VMware vCenter content library. You then upgrade by redeploying Cisco ACI Virtual Edge on the ESXi hosts.

You perform these upgrade tasks using the Cisco ACI vCenter plug-in only. You cannot use the VMware PowerCLI or a Python script.

The Cisco ACI vCenter plug-in was originally designed to work with Adobe Flash. However, and Adobe has deprecated flash in VMware vSphere version 6.7, and Adobe will stop updating Flash at the end of 2020. Beginning with the VMware vSphere 6.7 release, a new version—Cisco ACI HTML5 vCenter plug-in—designed to work with HTML5 is available. This section includes upgrade procedures for both plug-ins.

Note

- The name of the VMware vSphere client differs depending on whether you use the Flash or HTML5 version. The Flash version is referred to as the VMware vSphere Web Client; the HTML5 version is referred to as the VMware vSphere Client.
- Do not use the vSphere (thick) Client to upgrade Cisco ACI Virtual Edge or modify its vApp properties. Use only the Cisco ACI vCenter plug-in. Use only the vSphere Web Client to modify Cisco ACI Virtual Edge vApp properties.
- The Cisco ACI Virtual Edge upgrade gets stuck on hosts through the Cisco ACI fabric plug-in in VMware vCenter 7.0U1. It also fails to put the host into maintenance mode to install the new Cisco ACI Virtual Edge virtual machine (VM). This happens when you try to upgrade try Cisco ACI Virtual Edge on VMware vCenter 7.0U1 that has vSphere Custer Services (vCLS)-enabled VMs deployed in a cluster by default. Doing so is required for Distributed Resource Scheduler (DRS) and high availability.

  To remedy the issue, manually migrate the vCLS VMs from the host in the cluster where the Cisco ACI Virtual Edge VM upgrade is scheduled to any other host in the cluster.
- Migrate from Cisco Application Virtual Switch (AVS) to Cisco ACI Virtual Edge before upgrading to Cisco Application Policy Infrastructure Controller (APIC) 5.0(x) and later releases. Cisco AVS VMM domains are not supported beginning in Cisco APIC release 5.0(x).

The following sections provide information about prerequisites and installation.

For information about other Cisco Cisco ACI Virtual Edge tasks, see the following sections in this guide.

- Installing Cisco ACI Virtual Edge: See the chapter Cisco ACI Virtual Edge Installation, on page 9.
- Migrating from Cisco AVS to Cisco ACI Virtual Edge: See the chapter Migration from Cisco AVS to Cisco ACI Virtual Edge, on page 41.
- Migrating from VMware VDS to Cisco ACI Virtual Edge: See the chapter Migration from VMware VDS to Cisco ACI Virtual Edge, on page 49.

Recommended Upgrade Sequence for Cisco APIC, the Fabric Switches, and Cisco ACI Virtual Edge

When you upgrade the Cisco APIC, NX-OS software on the fabric switches, or Cisco ACI Virtual Edge, upgrade them all so they remain compatible.

To avoid network traffic disruption, we recommend that you perform the different upgrades in the following order:

Important Before you upgrade the Cisco APIC, fabric switches, and Cisco ACI Virtual Edge, check the *Cisco Application Policy Infrastructure Controller Release Notes* and the *Cisco ACI Virtual Edge Release Notes* for software compatibility information. All are available on Cisco.com.

1. The Cisco APIC software image—Follow the instructions in the *Cisco APIC Management, Installation, Upgrade, and Downgrade Guide*.

If you have Cisco APIC clusters, the clusters are upgraded one by one automatically.

2. The switch software on the fabric switches—Follow the instructions in the *Cisco APIC Management, Installation, Upgrade, and Downgrade Guide*.

   To avoid network traffic disruption during the upgrade, provide a path for Cisco ACI Virtual Edge traffic by putting the TORs and spines into different firmware or maintenance groups and then upgrading each firmware or maintenance group individually.

3. The Cisco ACI Virtual Edge—Complete the following tasks:

   a. Follow the instructions in this chapter.

   b. Complete one of the following steps:

      - Run the **vem restart** command on the VIBs if you decide to keep the VIBs on the current release.
      - Upgrade the VIBs to the later release if you decide to upgrade the VIBs.

Cisco ACI Virtual Edge Upgrade Workflow

This section provides a high-level description of the tasks required to upgrade the Cisco ACI Virtual Edge.

1. Fulfill all the prerequisites. See the section Prerequisites for Upgrading Cisco ACI Virtual Edge, on page 55 in this guide for instructions.
2. Download the Cisco ACI Virtual Edge Open Virtualization Format (OVF) file from Cisco.com and then upload it to the vCenter content library. See the section Upload the Cisco ACI Virtual Edge VM OVF File to the VMware vCenter, on page 56 in this guide for instructions.
3. Deploy Cisco ACI Virtual Edge on the ESXi hosts. See the section Upgrade Cisco ACI Virtual Edge Using the Flash Version of the Cisco ACI vCenter Plug-In, on page 58 in this guide for instructions.

Prerequisites for Upgrading Cisco ACI Virtual Edge

Perform the following tasks before you upgrade Cisco ACI Virtual Edge:

- Ensure that the Cisco ACI Virtual Edge that you plan to upgrade is properly configured and is operating without any issues.
- Check the Cisco ACI Virtual Edge Release Notes on Cisco.com for information about upgrading to the desired version.
- Ensure that OpFlex is online.
- In order to use the Cisco ACI vCenter plug-in, we recommend that you use vCenter 6.0 Update 3 or later.
- If you want to use the Cisco ACI vCenter plug-in to upgrade the Cisco ACI Virtual Edge, you first must upgrade the plug-in to the version shipped with the Cisco APIC version (4.x).
- If you use static or DHCP IP pools, ensure that you have enough IP addresses.

There must be more IP addresses in the static or DHCP pools than there are the in the Cisco ACI Virtual Edge service VMs in the data center in VMware vCenter. Otherwise, the upgrade of the new Cisco ACI Virtual Edge will fail.

- If the host is *not* part of a DRS cluster, manually move the non-Cisco ACI Virtual Edge VMs out of the host or power them off before the upgrade. If the host is part of a DRS cluster, non-Cisco ACI Virtual Edge VMs are moved out of the host automatically.

Cisco ACI Virtual Edge Upgrade

After you fulfill the upgrade prerequisites, you can use the Cisco Application Centric Infrastructure (ACI) Virtual Edge VMware vCenter to install . You use the Cisco ACI plug-in for VMware vCenter, which automates the process.

Note If you use a version of VMware vSphere earlier than 6.7, you use the Cisco ACI vCenter plug-in, which is designed to work with Flash. If you use VMware vSphere 6.7, you use the Cisco ACI HTML5 vCenter plug-in, which is designed to work with HTML5. This section provides procedures for both plug-ins.

You first upload the Cisco ACI Virtual Edge VM OVF file to the VMware vCenter content library. You can then deploy Cisco ACI Virtual Edge on the ESXi hosts.

Note If you use a local data store for content library storage, re-create the content library after you remove a host and then reattach it to vCenter. That is because the data store ID changes after the host is reattached, breaking the association between the content library and the data store.

Note After you deploy Cisco ACI Virtual Edge, do not remove it from the vCenter inventory and add it back. Doing so removes all the configurations you made during deployment. Deploy a new Cisco ACI Virtual Edge instead of adding an existing one back to the inventory.

Upload the Cisco ACI Virtual Edge VM OVF File to the VMware vCenter

You upload the Cisco ACI Virtual Edge VM OVF file to the VMware vCenter before you deploy Cisco ACI Virtual Edge on the ESXi hosts.

Before you begin

You must have done the following:

- Downloaded the folder with the OVF file to your computer.
- Check the Cisco ACI Virtual Edge Release Notes on Cisco.com to ensure that the OVF file is compatible with the version of Cisco APIC.
- Have already registered the Cisco ACI fabric inside the Cisco ACI vCenter plug-in.

Procedure

Step 1 Log in to the vSphere Web Client.

Step 2 Choose **Content Libraries**.

You can use an existing content library or create one to receive the upload of the Cisco ACI Virtual Edge VM OVF. See VMware documentation for instructions.

Step 3 Choose the library and then click **Import item**.

Step 4 In the **Import library item** dialog box, click the **Browse** button.

Step 5 In the pop-up dialog box, choose the OVF file and click **Open**.

Once the OVF file is uploaded to the content library, it appears in the work pane under the **Templates** tab.

Upgrade Cisco ACI Virtual Edge Using the HTML5 Version of the Cisco ACI vCenter Plug-in

After you upload a new Cisco Application Centric Infrastructure (ACI) Virtual Edge VM OVF file to the VMware vCenter, you upgrade by redeploying Cisco ACI Virtual Edge on the ESXi hosts.

Before you begin

You must have uploaded the Cisco ACI Virtual Edge VM OVF file to the VMware vCenter.

Procedure

Step 1 Log in to the VMware vSphere Client.

Step 2 On the **Home** page, in the left navigation pane, click **Cisco ACI Fabric**.

Step 3 In the **Cisco ACI Fabric** navigation pane, choose the fabric from the **Fabric** drop-down list.

Step 4 In the left navigation pane, click **AVE** to display the list of domains associated with the fabric, and then double-click the domain where you want to deploy the Cisco ACI Virtual Edge VM.

Step 5 In the **AVE** work pane, click the **AVE** tab.

Step 6 (Optional) In the upper right of the work pane, click **Max concurrent tasks** pencil icon to choose the number of deployments to run at the same time.

If you want to deploy the Cisco ACI Virtual Edge VM on multiple hosts, if you specify the number of concurrent tasks, the VM will be deployed on the number of hosts that you specify. For example, if you choose to deploy the VM on five hosts and choose three tasks to run concurrently, deployment will proceed on three of the hosts at the same time while deployment for the other two hosts is queued.

Step 7 In the **Datacenter** table, check the check box for each host on which you want to deploy the Cisco ACI Virtual Edge VM.

Step 8 Click **UPGRADE AVE**.

Step 9 In the pop-up window, click **CONTINUE**.
The **New AVE Wizard** appears.

Step 10 In the **Version** pane, click the radio button for the Cisco ACI Virtual Edge version that you want to use and then click **NEXT**.

Step 11 In the **Networking** pane, click the radio button for the management port group that you want to use with the Cisco ACI Virtual Edge VM and then click **NEXT**.

Step 12 In the **Storage** pane, complete one of the following actions:

- Leave the check box checked for **Let vCenter select the Datastore Automatically** and then click **NEXT**.

  Uncheck the check box for **Let vCenter select the Datastore Automatically**, from the host drop-down list, choose a datastore, and then click **NEXT**.

Step 13 In the **Settings** pane, in the **Admin Password** and the **Confirm Admin Password** fields, enter your password for the VMware vCenter and then click **NEXT**.

Step 14 In the **Summary** pane, view information about the newly deployed VM and then click **FINISH**.

What to do next

Verify that the upgrade is underway. In the **AVE** work pane, a **New AVE** pop-up window appears on the host where you deployed the VM. The host displays the percentage of how much of the upgrade has completed. You also can click the clipboard icon at the upper right of the work pane and in the **ACI Tasks & Settings**, view information about the **New AVE** task.

Upgrade Cisco ACI Virtual Edge Using the Flash Version of the Cisco ACI vCenter Plug-In

After you upload a new Cisco Application Centric Infrastructure (ACI) Virtual Edge VM OVF file to the VMware vCenter, you upgrade by redeploying Cisco ACI Virtual Edge on the ESXi hosts.

Before you begin

You must have uploaded the Cisco ACI Virtual Edge VM OVF file to the VMware vCenter.

Note If you use VMware vCenter 6.0 Web Client, the pop-up window for browsing to the OVF file may not appear. In that case, upload the OVF and virtual machine disk file (VMDK) to the HTTP server. Then use the OVF file URL from the server to download the OVF file to the content library.

Procedure

Step 1 Log in to the vSphere Web Client.

Step 2 In the **Home** work pane, click the **Cisco ACI Fabric** icon.

Step 3 In the **Cisco ACI Fabric** navigation pane, click **ACI Virtual Edge**.

Step 4 In the **ACI Virtual Edge** work pane, if there are multiple virtual domains, choose the domain from the **Select an ACI Virtual Edge Domain** drop-down list.

If there is only one virtual domain, skip to the next step.

Step 5 Choose the host or hosts on which you want to deploy Cisco ACI Virtual Edge.

Step 6 From the **ACI Virtual Edge version** drop-down list, choose the version to be deployed.

Step 7 From the **Management PortGroup** drop-down list, choose the management port group.

Step 8 From the **Datastore** drop-down list, choose **Custom**, click **Edit**.

Step 9 In the **Custom AVE Datastore selection** dialog box, choose a local or a remote data store for each Cisco ACI Virtual Edge.

Note To ensure a higher level of availability, we recommend that you choose a local data store if you have one.

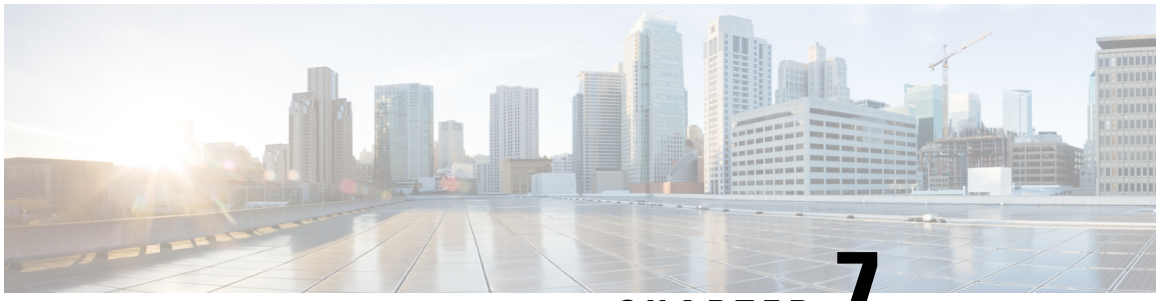
Note You may not see all types of local storage in vCenter. However, if you uncheck the **Use local datastore only** check box, vCenter shows all local data stores. For details, see the documentation on the VMware website for details.

Step 10 In the **VM Admin Password** fields, enter a new password for the Cisco ACI Virtual Edge VMs.

Step 11 Click **Install/Upgrade ACI Virtual Edge**.

Step 12 In the dialog box, click **Yes**.

In the work pane, the installed hosts display OpFlex status, the Cisco ACI Virtual Edge VM, and management IP. It could take a little while for OpFlex to come up.



CHAPTER 7

Cisco ACI Virtual Edge Uninstallation

This chapter describes uninstallation of Cisco ACI Virtual Edge, including prerequisites and uninstallation methods.

About Cisco ACI Virtual Edge Uninstallation

You might need to remove Cisco Application Centric Infrastructure (ACI) Virtual Edge for testing or if you need to remove all configuration from the Cisco ACI fabric, resetting the fabric to its initial state.

You can uninstall Cisco ACI Virtual Edge by using the Cisco ACI plug-in for VMware vCenter, the VMware PowerCLI, or a Python script.

The Cisco ACI vCenter plug-in was originally designed to work with Adobe Flash. However, at the end of 2020, Adobe will stop updating Flash. Beginning with the VMware vSphere 6.7 release, the Flash version of the plug-in is deprecated. Instead, VMware vSphere 6.7 uses a new version—Cisco ACI HTML5 vCenter plug-in—is designed to work with HTML5. This section includes uninstallation procedures for both plug-ins.

Note The name of the VMware vSphere client differs depending on whether you use the Flash or HTML5 version. The Flash version is referred to as the VMware vSphere Web Client; the HTML version is referred to as the VMware vSphere Client.

Note In order to use the Cisco ACI Virtual Edge management tools (the ACI vCenter plug-in, the VMware PowerCLI, and Python scripts), we recommend that you use vCenter 6.0 Update 3 or later.

Workflow for Uninstalling Cisco ACI Virtual Edge

The order of tasks that you perform to uninstall Cisco ACI Virtual Edge depends on whether you want to keep using the VMM domain after uninstallation.

- To remove Cisco ACI Virtual Edge and keep using the VMM domain (in native mode):
  1. Remove all VMs from Cisco ACI Virtual Edge port groups.

     Alternatively, change the switching mode of the Cisco ACI Virtual Edge EPGs from AVE to native.
  2. Uninstall the Cisco ACI Virtual Edge VM, using the Cisco ACI vCenter plug-in, VMware PowerCLI, or a Python script. Follow the instructions in this guide.

- To remove Cisco ACI Virtual Edge and delete the VMM domain:
  1. Remove all VMs from EPG port groups.
  2. Uninstall the Cisco ACI Virtual Edge VM, using the Cisco ACI vCenter plug-in, VMware PowerCLI, or a Python script. Follow the instructions in this guide.
  3. Remove all hosts from the Cisco ACI Virtual Edge VDS.
  4. Remove all VMM domain associations to EPGs to delete port groups.
  5. Remove the Cisco ACI Virtual Edge VMM domain.

Uninstall Cisco ACI Virtual Edge Using the HTML5 Version of the Cisco ACI vCenter Plug-in

You can remove the Cisco Application Centric Infrastructure (ACI) Virtual Edge from a host by using the HTML5 version of the Cisco Application Centric Infrastructure (ACI) vCenter plug-in.

Procedure

Step 1 Log in to the VMware vSphere Client.

Step 2 On the **Home** page, in the left navigation pane, click **Cisco ACI Fabric**.

Step 3 In the **Cisco ACI Fabric** navigation pane, choose the fabric from the **Fabric** drop-down list.

Step 4 In the left navigation pane, click **AVE** to display the list of domains associated with the fabric, and then double-click the domain from which you want to remove the Cisco ACI Virtual Edge VM.

Step 5 In the **AVE** work pane, click the **AVE** tab.

Step 6 (Optional) In the upper right of the work pane, click **Max concurrent tasks** pencil icon to choose the number of deployments to run at the same time.

If you want to remove the Cisco ACI Virtual Edge VM from multiple hosts, if you specify the number of concurrent tasks, the VM will be removed from the number of hosts that you specify. For example, if you choose to remove the VM on five hosts and choose three tasks to run concurrently, removal will proceed on three of the hosts at the same time while removal for the other two hosts is queued.

Step 7 In the **Datacenter** table, check the check box for each host from which you want to remove the Cisco ACI Virtual Edge VM.

Step 8 Click **REMOVE AVE**.

The **REMOVE AVE** wizard appears.

Step 9 In the **Summary** pane, make sure that the **Enter Maintenance Mode** check box is checked, and then click **FINISH**.

Note We recommend putting the host in maintenance mode before you click **FINISH** and uninstall Cisco ACI Virtual Edge if you have a DRS cluster where other hosts have VMs using Cisco ACI Virtual Edge. Going into maintenance mode prevents other VMs from migrating to the host after Cisco ACI Virtual Edge is uninstalled. If there are no other hosts in the cluster where VMs use Cisco ACI Virtual Edge, then you can proceed with uninstallingCisco ACI Virtual Edge without putting the host in maintenance mode.

What to do next

Verify that the removal is underway. In the **AVE** work pane, a In the **AVE** work pane, a **Remove AVE** pop-up window appears on the host where you removed the VM. The host displays the percentage of how much of the removal has completed. You also can click the clipboard icon at the upper right of the work pane and in the **ACI Tasks & Settings**, view information about the **Remove AVE** task.

Uninstall Cisco ACI Virtual Edge Using the Flash Version of the Cisco ACI vCenter Plug-in

Note We recommend putting the host in maintenance mode before you uninstall Cisco ACI Virtual Edge if you have a DRS cluster where other hosts have VMs using Cisco ACI Virtual Edge. Going into maintenance mode prevents other VMs from migrating to the host after Cisco ACI Virtual Edge is uninstalled. If there are no other hosts in the cluster where VMs use Cisco ACI Virtual Edge, then you can proceed with uninstalling Cisco ACI Virtual Edge without putting the host in maintenance mode.

Procedure

Step 1 Log in to VMware vSphere Web Client.

Step 2 Choose **Cisco ACI Fabric** > **ACI Virtual Edge**.

Step 3 At the top of the central work pane, from the **Select an ACI Virtual Edge Domain** drop-down list, choose a domain.

When you choose a domain, the work pane displays the host or hosts in the vCenter related to the VMM domain.

Step 4 Choose one or more hosts by clicking the appropriate check box or check boxes.

Step 5 Below the **Uninstall ACI Virtual Edge** button, if you chose multiple hosts in Step 4, choose how many hosts on which to uninstall Cisco ACI Virtual Edge at the same time using the + and - buttons.

Step 6 Click **Uninstall ACI Virtual Edge**.

Step 7 In the **Uninstall AVE** dialog box, click Yes to confirm you wish to proceed with uninstalling Cisco ACI Virtual Edge.

If any of the selected hosts are part of a DRS cluster, a warning popup appears, asking if you agree to have the hosts put in maintenance mode as part of the uninstallation.

Step 8 Complete one of the following sets of actions:

If you...	Then...
Want to proceed with the uninstallation with the hosts put in maintenance mode	Click **Yes**.
Want to proceed with the uninstallation but not put the hosts in maintenance mode	Click **No**. An additional warning displays, asking you to confirm: • Click **Yes** to proceed with uninstallation without putting the hosts in maintenance mode. • Click **No** to cancel the uninstallation.
Do not want to proceed with the uninstallation	Click **No** to cancel the uninstallation.

In the central work pane, the **Status** column for the host displays the uninstallation progress. You also can view progress of the individual uninstallation tasks in the **Recent Tasks** area. When uninstallation is complete, **Not installed** appears in the **Status** column for the host.

What to do next

If the host is part of a DRS cluster, do not move it out of maintenance mode unless it has been removed from the Cisco ACI Virtual Edge DVS.

Uninstall Cisco ACI Virtual Edge Using the VMware PowerCLI

If you have a Windows platform, you can use the VMware PowerCLI to uninstall Cisco Application Centric Infrastructure (ACI) Virtual Edge.

Before you begin

The script check for any existing data virtual machines (VMs) still dependent on the Cisco ACI Virtual Edge VM. Remove all data VMs from the Cisco ACI Virtual Edge DVS before deleting the Cisco ACI Virtual Edge VM.

Procedure

Uninstall Cisco ACI Virtual Edge using the **Remove-AveVM** command.

The following text shows the command syntax:

```
Remove-AveVM [[-HostName] Object] [[-DomainName] Object] [CommonParameters]
```

Example:

```
PowerCLI C:\> Remove-AveVM -HostName 172.23.143.129 -DomainName mininet
```

Output with maintenance mode:

```
Connecting to vCenter.....................................................[ok]
Fetching existing AVE VM..................................................[ok]
The Host 172.23.143.129 is part of a DRS enabled cluster (cluster).
The uninstall procedure will place the host in maintenance mode in order to avoid hav
ing DRS automatically migrate Virtual Machine to this host.
Do you wish to continue? [yes/no]: yes
Validating DRS cluster cluster............................................[ok]
Adding affinity rule on DRS cluster cluster...............................[ok]
Waiting for all VMs to move out of host 172.23.143.129.....................[ok]
Powering off the AVE VM...................................................[ok]
Deleting VM...............................................................[ok]
Entering maintenance mode.................................................[ok]
Removing affinity rule on DRS cluster.....................................[ok]
Cleaning up...............................................................[ok]
```

Output without maintenance mode:

```
Connecting to vCenter.....................................................[ok]
Fetching existing AVE VM..................................................[ok]
The Host 172.23.143.129 is part of a DRS enabled cluster (cluster).
The uninstall procedure will place the host in maintenance mode in order to avoid hav
ing DRS automatically migrate Virtual Machine to this host.
Do you wish to continue? [yes/no]: no
Do you wish to cancel the uninstall, or continue the uninstall without placing the ho
st in maintenance mode (not recommended) [cancel/continue]: continue
Deleting VM...............................................................[ok]
Cleaning up...............................................................[ok]
```

Uninstall Cisco ACI Virtual Edge Using Python

You can uninstall Cisco Application Centric Infrastructure (ACI) Virtual Edge using a Python script.

Before you begin

The script checks for any existing data virtual machines (VMs) still dependent on the Cisco ACI Virtual Edge VM. Remove all data VMs from the Cisco ACI Virtual Edge VM before deleting the Cisco ACI Virtual Edge VM.

Procedure

Uninstall Cisco ACI Virtual Edge from a given host for a given domain using the `remove-avevm.py` script.

The following text shows the script usage:

```
usage: remove-avevm.py [-h] [--silent] --vcenter VCENTER --vc-username
VC_USERNAME [--vc-password VC_PASSWORD] --host-name
```

```
HOST_NAME --domain-name DOMAIN_NAME
[--ignore-active-vm]
```

Example:

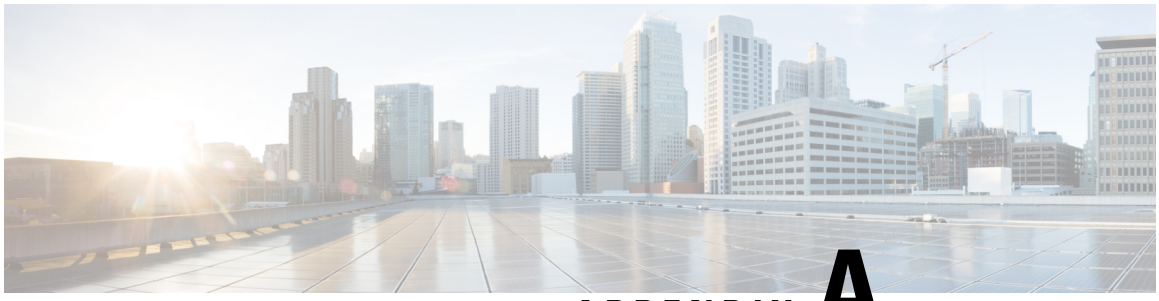
```
(venv) $ python remove-avevm.py --vcenter 172.23.143.235 --vc-username admin
--vc-password lab --host-name 172.23.143.129 --domain-name mininet
```

Output with maintenance mode:

```
Connecting to vCenter.....................................................[ok]
Fetching existing AVE VM..................................................[ok]
The Host 172.23.143.129 is part of a DRS enabled cluster (cluster).
The uninstall procedure will place the host in maintenance mode in order to avoid hav
ing DRS automatically migrate Virtual Machine to this host.
Do you wish to continue? [yes/no]: yes
Validating DRS cluster cluster............................................[ok]
Adding affinity rule on DRS cluster cluster...............................[ok]
Waiting for all VMs to move out of host 172.23.143.129.....................[ok]
Powering off the AVE VM...................................................[ok]
Deleting VM...............................................................[ok]
Entering maintenance mode.................................................[ok]
Removing affinity rule on DRS cluster.....................................[ok]
Cleaning up...............................................................[ok]
```

Output without maintenance mode:

```
Connecting to vCenter.....................................................[ok]
Fetching existing AVE VM..................................................[ok]
The Host 172.23.143.129 is part of a DRS enabled cluster (cluster).
The uninstall procedure will place the host in maintenance mode in order to avoid hav
ing DRS automatically migrate Virtual Machine to this host.
Do you wish to continue? [yes/no]: no
Do you wish to cancel the uninstall, or continue the uninstall without placing the ho
st in maintenance mode (not recommended) [cancel/continue]: continue
Deleting VM...............................................................[ok]
Cleaning up...............................................................[ok]
```



APPENDIX A

Supported Topologies

This appendix provides information about the topologies supported for the Cisco ACI Virtual Edge.

Important *Topologies not included in this appendix have not been tested and are not supported.*

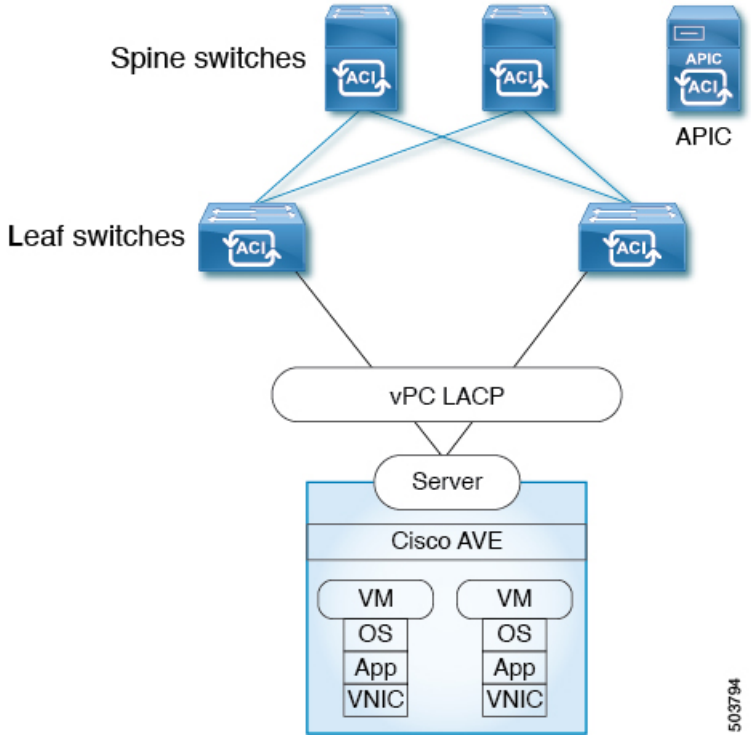
Note For all topologies, we recommend using LACP wherever possible and supported by your hardware. We recommend using MAC pinning only when using LACP is not possible.

For a given ESXi host, that host can only be connected to a single pair of leaves in a vPC domain. This means in the case of a blade enclosure like a UCS B Series Chassis with Fabric Interconnects (FI), the fabric interconnects must be connected to the same vPC domain.

Direct Connection

This topology connects the ESXi hypervisor to the Cisco Application Centric Infrastructure Controller directly.

Figure 4: Direct Connection



To use this topology, you must configure port channel policy both under **Fabric** > **Access Policies** and when you create the Cisco Application Centric Infrastructure (ACI) Virtual Edge virtual machine manager (VMM) domain. See the following procedures:

- Configure a Port Channel or Virtual Port Channel Using the GUI in the *Cisco ACI Virtual Edge Configuration Guide*
- Create a VMM Domain Profile for Cisco ACI Virtual Edge , on page 82 in this guide.

Alternatively, you can configure the VMM domain profile using the configuration wizard under the **Fabric** wizard. If you do so, you do not need to configure the port channel using the procedure in the *Cisco ACI Virtual Edge Configuration Guide*.

Note Do not use MAC pinning with a direct connection to a VPC leaf pair. Instead, use Link Aggregation Control Protocol (LACP) or enhanced LACP to provide redundancy and reliability. Using MAC pinning with a direct connection leads to traffic loss when peer leaf switches are rebooted. Use MAC Pinning only where virtual port channel (VPC) cannot be supported, such as for Cisco UCS Fabric Interconnects with southbound interfaces.

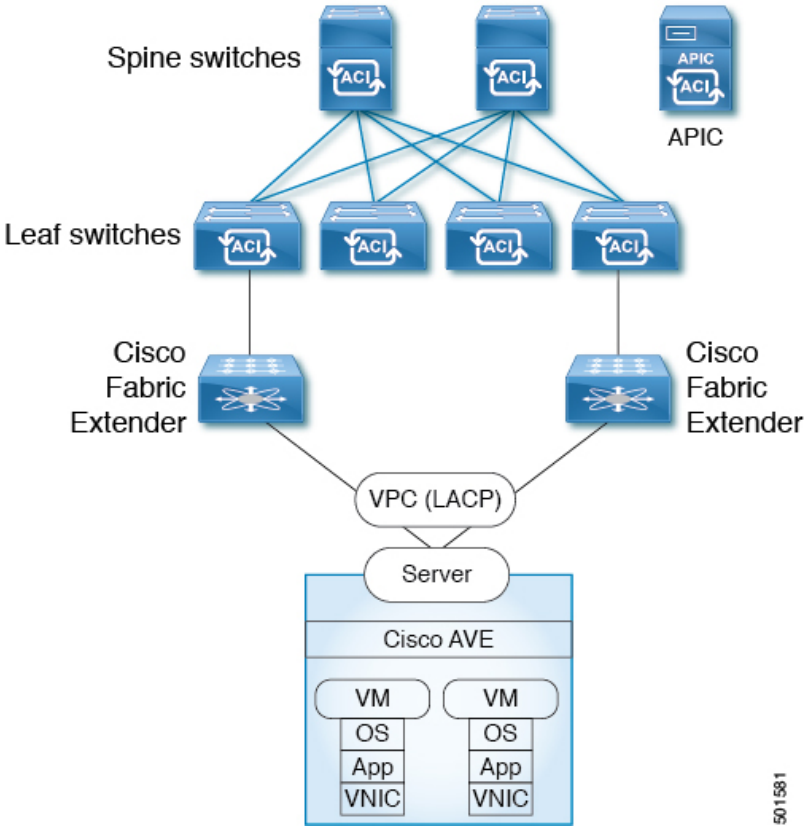
Cisco Fabric Extender

This topology connects the ESXi hypervisor to the Cisco APIC through a Fabric Extender (FEX). You can connect the ESXi to the following:

- Multiple leaf switches using a virtual port channel (VPC)
- A single leaf switch using a port channel (MAC pinning or LACP bundle)

In the following illustration, VPC is used as an example. You can use port channel instead.

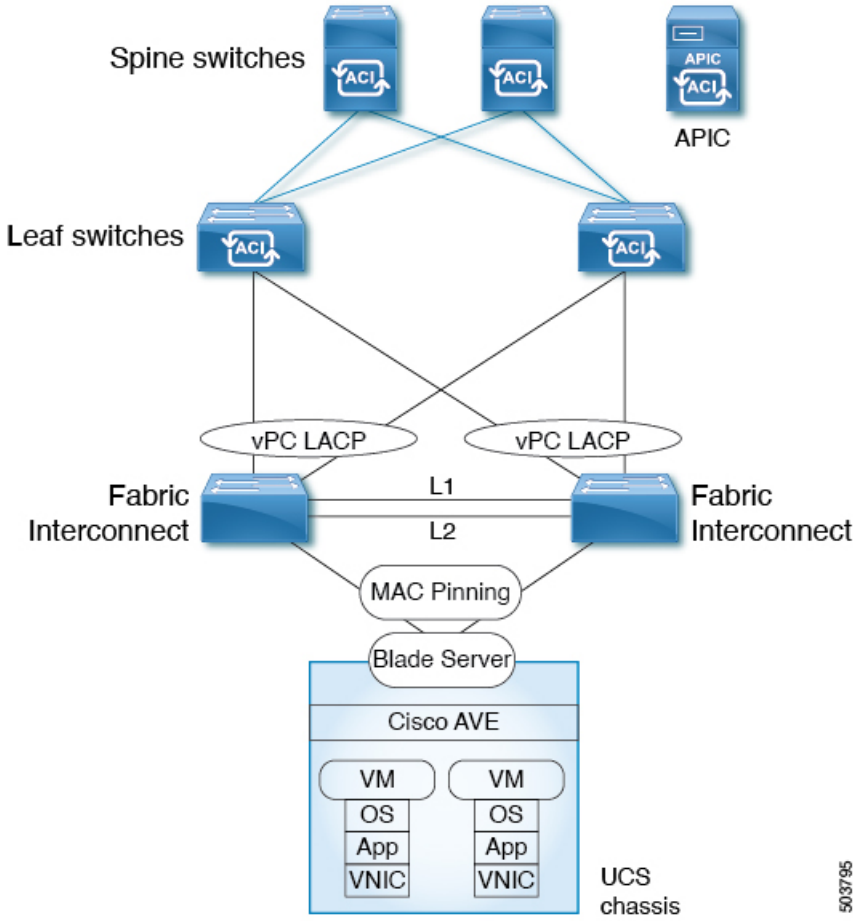
Figure 5: Cisco Fabric Extender Topology



VPC with Cisco UCS Fabric Interconnects

This topology connects the ESXi hypervisor to the Cisco APIC using Cisco UCS Fabric Interconnects, VPCs, LACP, and MAC pinning.

Figure 6: VPC with Cisco UCS Fabric Interconnects Topology

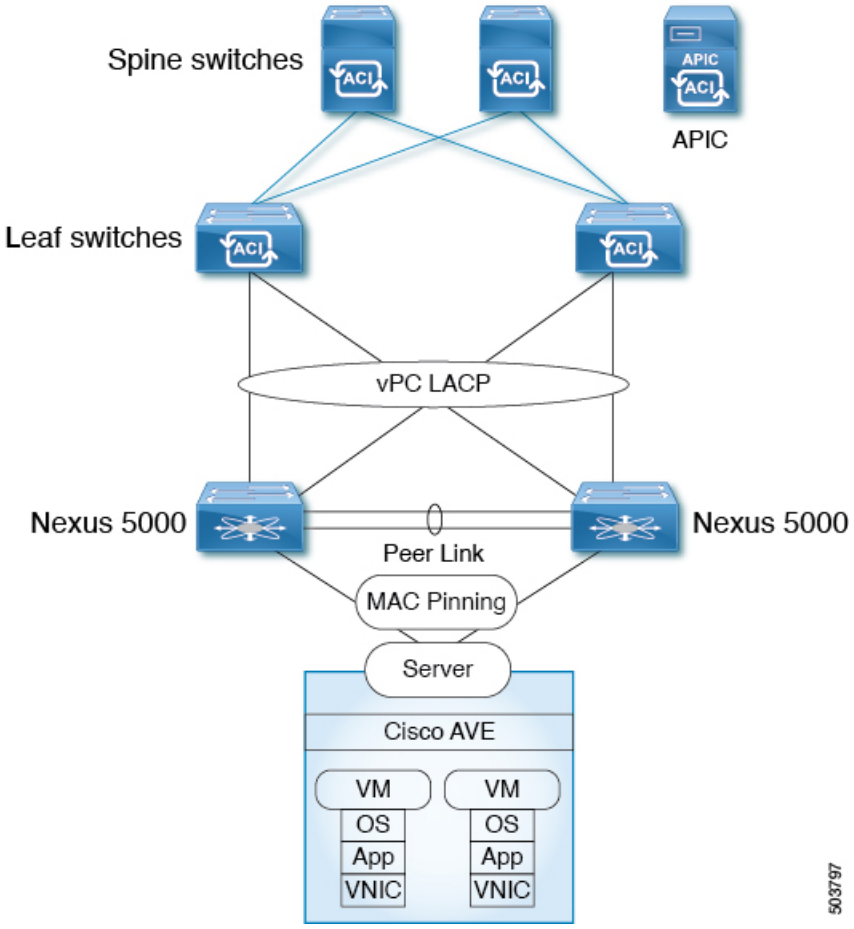


In this topology, the Cisco ACI Virtual Edge can be configured only with MAC pinning. That is because Cisco UCS Fabric Interconnects don't support LACP or vLACP on the southbound ports towards the blade server. Therefore, the illustration shows MAC pinning only on the Cisco ACI Virtual Edge side. Each UCS Fabric Interconnect has a vPC Port-Channel to the same pair of leafs in a vPC Domain.

Dual-Side VPC with Cisco Nexus 5000 and MAC Pinning

This topology connects the ESXi hypervisor to a Cisco Application Policy Infrastructure Controller (APIC) through the Cisco Nexus 5000 switch, virtual port channels, and MAC pinning.

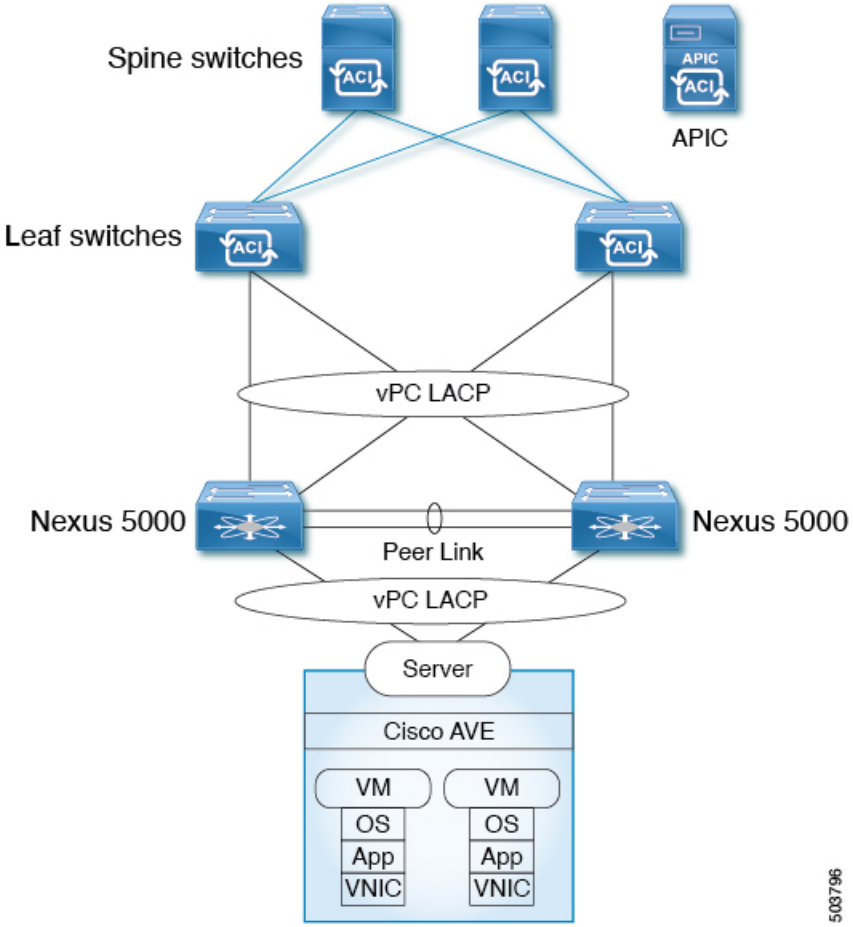
Figure 7: Dual-Side VPC with Cisco Nexus 5000 and MAC Pinning Topology



Dual-Side VPC with Cisco Nexus 5000 and VPC

This topology connects the ESXi hypervisor to a Cisco Application Policy Infrastructure Controller (APIC) through the Cisco Nexus 5000 switch and virtual port channels.

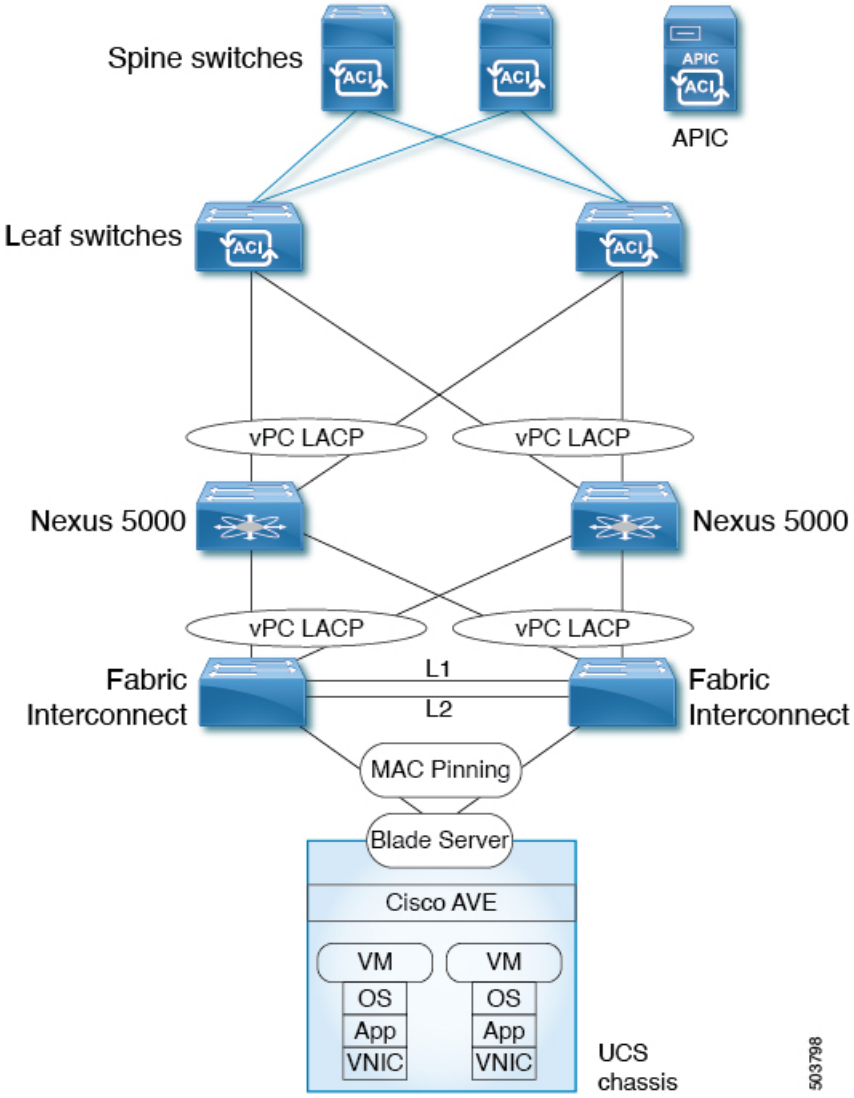
Figure 8: Dual-Side VPC with Cisco Nexus 5000 and VPC Topology



Single-Side VPC with Cisco Nexus 5000 and Cisco UCS Fabric Interconnects

This topology connects the ESXi hypervisor to the leaf switches using MAC pinning, directly or through Cisco Nexus 5000 switches and Cisco UCS Fabric Interconnects.

Figure 9: Single-Side VPC with Cisco Nexus 5000 and Cisco UCS Fabric Interconnects Topology

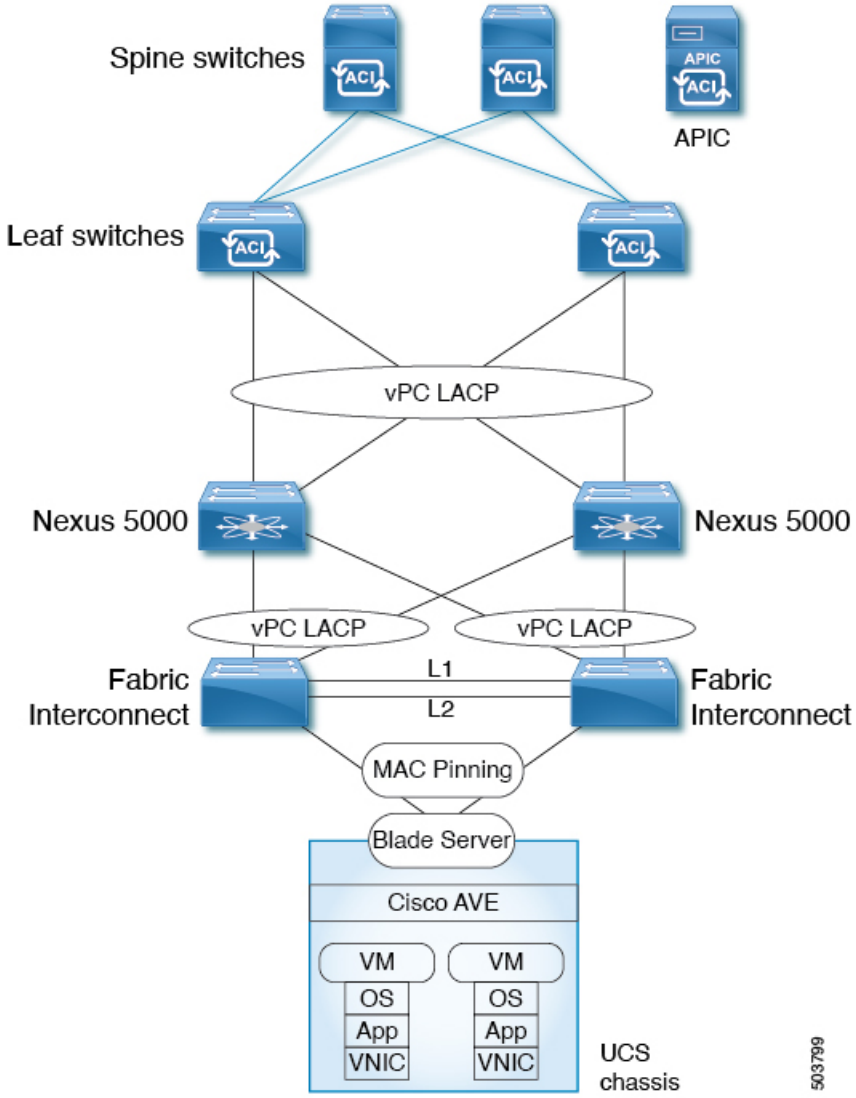


In this topology, the Cisco ACI Virtual Edge can be configured only with MAC pinning. That is because Cisco UCS Fabric Interconnects do not support LACP on the southbound ports toward the blade server. Therefore, the illustration shows MAC pinning only on the Cisco ACI Virtual Edge side.

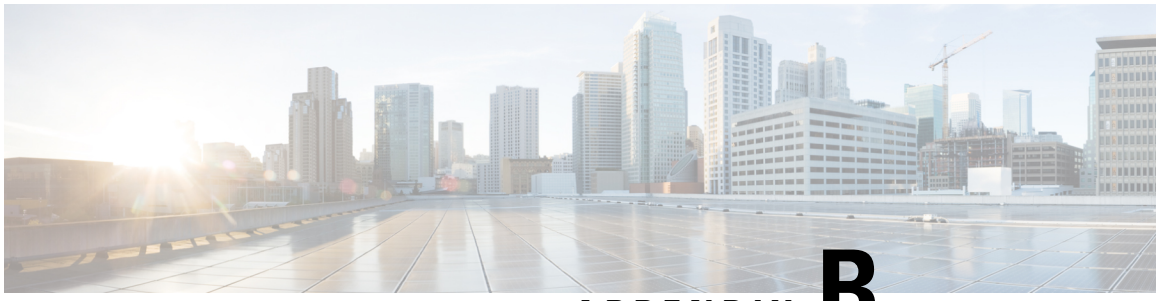
Dual-Side VPC with Cisco Nexus 5000 and Cisco UCS Fabric Interconnects

This topology connects the ESX hypervisor to the leaf switches using MAC pinning, directly or through Cisco Nexus 5000 switches and Cisco UCS Fabric Interconnects.

Figure 10: Dual-Side VPC with Cisco Nexus 5000 and Cisco UCS Fabric Interconnects Topology



In this topology, the Cisco ACI Virtual Edge can be configured only with MAC pinning. That is because Cisco UCS Fabric Interconnects do not support LACP on the southbound ports toward the blade server. Therefore, the illustration shows MAC pinning only on the Cisco ACI Virtual Edge side.



APPENDIX B

Alternate Procedures for Creating vCenter Domain, Interface, and Switch Profiles

We recommend using the unified configuration wizard for performing configuration tasks before installing Cisco ACI Virtual Edge. However, you may need to configure separate, more detailed policies.

This appendix includes individual procedures for creating a vCenter domain profile and different kinds of interface and switch profiles:

Create Port Channel Switch and Interface Profiles

Before you can install Cisco ACI Virtual Edge, create switch and interface profiles.

Before you begin

In Step 4 d of this procedure, you choose a leaf switch node ID from the drop-down list. It must match the node ID of the leaf switch connected to the ESXi or Layer 2 cloud host. Check the leaf switch node ID in the **Fabric Membership** window by going to **Fabric** > **Inventory** > **Fabric Membership**.

Procedure

Step 1 Log in to the Cisco APIC.

Step 2 Choose **Fabric** > **Access Policies**.

Step 3 In the **Policies** navigation pane, expand the **Switches** folder and the **Leaf Switches** folder.

Step 4 Right-click the **Profiles** folder, and then choose **Create Leaf Profile**.

Step 5 In the **Create Leaf Profile (STEP 1 > Profile)** dialog box, complete the following steps:

a) In the **Name** field, enter a name.

b) In the **Leaf Selectors** field, click the + icon to create a new switch selector.

c) In the **Name** field, enter a name.

d) In the **Blocks** field, choose a leaf switch node ID from the drop-down list.

e) Click **Update**.

f) Click **Next**.

Step 6 In the **Create Leaf Profile (STEP 2 > Associations)** dialog box, in the **Interface Selectors Profiles** area, click the + icon to create a new interface selector profile.

Step 7 In the **Create Interface Profile** dialog box, complete the following steps:

a) In the **Name** field, enter the vLeaf name.

b) In the **Interface Selectors** area, click the + icon to create a new interface selector.

Step 8 In the **Create Access Port Selector** dialog box, complete the following steps:

a) Enter a name for the selector in the **Name** field.

b) In the **Interface IDs** field, enter the access port interface IDs for the physical interfaces connected to the ESXi host.

c) In the **Interface Policy Group** drop-down list, choose **Create PC Interface Policy Group**.

Step 9 In the **Create PC Interface Policy Group** dialog box, enter the policy group name in the **Name** field.

Step 10 In the **Port Channel Policy** field, choose **Create Port Channel Policy** from the drop-down list.

Step 11 In the **Create Port Channel Policy** dialog box, complete the following steps:

a) Enter the policy name in the **Name** field.

b) In the **Mode** field, choose one of the following values:

- **Static Channel - Mode On**
- **LACP Active**
- **LACP Passive**
- **MAC Pinning**
- **MAC Pinning-Physical-NIC-load**

Note Do not use MAC pinning with a direct connection to a VPC leaf pair. Instead, use Link Aggregation Control Protocol (LACP) or enhanced LACP to provide redundancy and reliability. Using MAC pinning with a direct connection leads to traffic loss when peer leaf switches are rebooted. Use MAC Pinning only where virtual port channel (VPC) cannot be supported, such as for Cisco UCS Fabric Interconnects with southbound interfaces.

c) Click **Submit**.

Step 12 In the **Create PC Interface Policy Group** dialog box, complete the following steps:

a) In the **Attached Entity Profile** field, choose a profile you created earlier or create one from the drop-down list.

b) Click **Submit**.

Step 13 In the **Create Access Port Selector** dialog box, click **OK**.

Step 14 In the **Create Leaf Interface Profile** dialog box, click **Submit**.

Step 15 In the **Create Leaf Profile** dialog box, choose the new interface profile and then click **Finish**.

Create VPC Interface and Switch Profiles Using the GUI

Procedure

Step 1 Log in to the Cisco APIC.

Step 2 Choose **Fabric** > **Access Policies**.

Step 3 In the **Policies** navigation pane, expand the **Policies** and **Switch** folders.

Step 4 Right-click the **VPC Domain** folder and choose **Create VPC Domain Policy**.

Step 5 In the **Create VPC Domain Policy** dialog box, complete the following steps:

a) In the **Name** field, enter a name for the policy.

b) In the **Peer Dead Interval** field, enter a value.

The range is from 3 seconds to 300 seconds.

c) Click **Submit** to save the policy.

Step 6 In the **Policies** navigation pane, expand the **Switches** and **Leaf Switches**folders, right-click the **Profiles** folder and choose **Create Leaf Profile**.

Step 7 In the **Create Leaf Profile** dialog box, complete the following steps:

a) In the **Name** field, enter a name for the profile.

b) In the **Leaf Selectors** area, click the + icon.

c) In the **Name** field, enter a switch selector name.

d) From the **Blocks** drop-down list, choose a leaf to be associated with a policy group.

e) Click **Update**.

f) Click **Next**.

Step 8 In the **Create Leaf Profile** dialog box, in the **Interface Selector Profiles** area, click the + icon.

Step 9 In the **Create Leaf Interface Profile** dialog box, complete the following steps:

a) In the **Name** field, enter a name for the profile.

b) In the **Interface Selectors** area, click the + icon.

Step 10 In the **Create Access Port Selector** dialog box, complete the following actions:

a) In the **Name** field, enter a selector name.

b) In the **Interface IDs** field, enter a range value.

c) From the **Interface Policy Group** drop-down list, choose **Create VPC Interface Policy Group** from the drop-down list.

Step 11 In the **Create VPC Interface Policy Group** dialog box, complete the following steps:

a) In the **Name** field, enter a name for the policy group.

b) From the **Port Channel Policy** drop-down list, choose **Create Port Channel Policy** from the drop-down list.

Step 12 In the **Create Port Channel Policy** dialog box, complete the following actions:

a) In the **Name** field, enter a name for the policy.

b) In the **Mode** field, choose one of the following options appropriate to your setup:

- **Static Channel - Mode On**

Alternate Procedures for Creating vCenter Domain, Interface, and Switch Profiles

- **LACP Active**
- **LACP Passive**
- **MAC Pinning**
- **MAC Pinning-Physical-load**

Note Do not use MAC pinning with a direct connection to a VPC leaf pair. Instead, use Link Aggregation Control Protocol (LACP) or enhanced LACP to provide redundancy and reliability. Using MAC pinning with a direct connection leads to traffic loss when peer leaf switches are rebooted. Use MAC Pinning only where virtual port channel (VPC) cannot be supported, such as for Cisco UCS Fabric Interconnects with southbound interfaces.

c) Click **Submit**.

Step 13 In the **Create VPC Interface Policy Group** dialog box, complete the following actions:

a) In the **Attached Entity Profile** field, choose **default** from the drop-down list.

You can create a new attachable entity profile to override policy after you create the node policy. You may need to do so if you have intermediate Layer 2 devices between the leaf and ESXi hosts that are running the Cisco ACI Virtual Edge and if you want to use LACP with the top of rack (TOR) switch/leafs on the fabric side but use another policy, such as MAC pinning, on the Cisco ACI Virtual Edge side.

b) Click **Submit**.

Step 14 In the **Create Access Port Selector** dialog box, click **OK**.

Step 15 In the **Create Leaf Interface Profile** dialog box, click **Submit**.

Step 16 In the **Create Leaf Profile** dialog box, complete the following steps:

a) In the **Interface Selector Profiles** area, check the check box for the interface selector profile that you created in Step 9 a.

b) Click **Finish**.

Step 17 To add a second leaf to the VPC, complete the following steps:

a) Repeat Step 1 through Step 10 b; however at Step 7 b, enter the node ID of the other leaf.

b) In the **Create Access Port Selector** dialog box, choose the name of the policy group that you created in Step 11 a.

c) Click **OK**.

d) Repeat Step 15 and Step 16.

Step 18 In the **Policies** navigation pane, expand the **Policies** and **Switch** folders.

Step 19 Right-click **Virtual Port Channel default**, and then choose **Create VPC Explicit Protection Group**.

Step 20 In the **Create VPC Explicit Protection Group** dialog box, enter a name, ID, and switch values for the protection group. Click **Submit** to save the protection group.

Note Each pair of leaf switches has one VPC Explicit Protection Group with a unique ID.

Note The same virtual port channel policy can contain multiple VPC explicit protection groups.

Create FEX Node Interface and Switch Profiles Using the GUI

Note If you have a FEX directly connected to a leaf, see the section "Cisco Fabric Extender" in the Topology appendix of this guide for information about limitations.

Before you begin

In Step 4 d of this procedure, you choose a leaf switch node ID that is connected with the FEX from the drop-down list. It must match the node ID of the leaf switch connected to the ESXi or Layer 2 cloud host. Check the leaf switch node ID in the **Fabric Membership** window by going to **Fabric** > **Inventory** > **Fabric Membership**.

Procedure

Step 1 Log in to the Cisco Application Policy Infrastructure Controller (APIC).

Step 2 Choose **Fabric** > **Access Policies**.

Step 3 In the **Policies** navigation pane, expand the **Switches** and **Leaf Switches** folders.

Step 4 Right-click the **Profiles** folder, and then choose **Create Leaf Profile**.

Step 5 In the **Create Leaf Profile STEP 1 > Profile** dialog box, complete the following steps:

a) In the **Name** field, enter a profile name.
b) In the **Leaf Selectors** field, click the + icon.
c) In the **Name** field, enter a name.
d) In the **Blocks** field, choose a leaf switch node ID that is connected with the FEX from the drop-down list.
e) Click on the **Blocks** drop-down arrow or anywhere on the **Create Switch Profile** dialog box so you can see the **Update** button.
f) Click **Update**.
g) Click **Next**.

Step 6 In the **Create Leaf Profile STEP 2 > Associations** dialog box, in the **Interface Selectors Profiles** area, click the + icon to create a new interface selector profile.

Step 7 In the **Create Leaf Interface Profile** dialog box, complete the following steps:

a) In the **Name** field, enter the vLeaf name.
b) In the **Interface Selectors** area, click the + icon to create a new interface selector.

Step 8 In the **Create Access Port Selector** dialog box, complete the following steps:

a) Enter a name for the selector in the **Name** field .
b) In the **Interface IDs** field, enter the access port interface IDs on the leaf that is connected to the FEX.
c) Check the **Connected To Fex** check box.
d) From the **FEX Profile** drop-down list, choose **Create FEX profile**.

Step 9 In the **Create FEX Profile** dialog box, complete the following steps:

a) In the **Name** field, enter an FEX profile name.
b) In the **FEX Access Interface Selectors** area, click the + icon to specify the FEX access ports.

Step 10 In the **Create Access Port Selector** dialog box, complete the following steps:

a) In the **Name** field, enter a selector name.
b) In the **Interface IDs** area, specify the access ports on the FEX that are connected to the ESXi server hosting the Cisco ACI Virtual Edge.
c) In the **Interface Policy Group** area, choose an option from the drop-down list.

You can choose **Create PC Interface Policy Group**, **Create VPC Interface Policy Group**, or **Create Leaf Access Port Policy Group**.

Step 11 In the dialog box for the option that you chose in Step 10c, complete the following steps:

a) In the **Name** field, enter an access policy group name.
b) In the **Attached Entity Profile** area, choose the appropriate attached entity profile.
c) Click **Submit**.

Step 12 In the **Create Access Port Selector** dialog box, verify that the newly created access port policy group appears in the **Interface Policy Group** area, and then click **OK**.

Step 13 In the **Create FEX Profile** dialog box, verify that the newly created FEX access interface selector profile appears in the **FEX Access Interface Selectors** area, and then click **Submit**.

Step 14 In the **Create Access Port Selector** dialog box, complete the following steps:

a) Verify that the newly created FEX profile appears in the **FEX Profile** area.
b) Enter an ID in the**FEX ID** field.
c) Click **OK**.

Step 15 In the **Create Leaf Interface Profile** dialog box, verify that the leaf-side interface port selector profile is present, and then click **Submit**.

Step 16 In the **Create Leaf Profile STEP 2 > Associations** dialog box, in the **Interface Selector Profiles** area, check the check box for the interface selector profile that you created for the FEX, and then click **Finish**.

What to do next

You should verify that the FEX node policy configuration was successful. However, you need to wait about 10 minutes to give the Cisco APIC time to complete the configuration.

To verify the FEX node policy configuration, complete the following steps in the Cisco APIC GUI:

1. Choose **Fabric** > **Inventory**.
2. In the **Inventory** navigation pane, expand the folder for the pod containing the leaf node for which the FEX node profile was created.
3. Expand the folder for the leaf node.
4. Choose the **Fabric Extenders** folder.
5. In the **Fabric Extenders** work pane, ensure that the FEX is present.

Modify the Interface Policy Group to Override vSwitch-Side Policies

After you create a node policy, you may need to create your own attachable entity profile. This may be necessary if you have intermediate Layer 2 devices between the leaf and ESXi hosts that are running the Cisco ACI Virtual Edge. Such devices include the Cisco Nexus 5000/7000 series switches or blade servers (Unified Computing System [UCS].

The override allows a separate link policy to be configured for the intermediate devices and for the Cisco ACI Virtual Edge host uplinks. For example, if you have UCS Fabric Interconnects connected to ACI, and your Cisco ACI Virtual Edge hosts are running on UCS blades, you may want the UCS Fabric Interconnect uplinks for each FI channeled using Port Channel policy, but the host vNICs for the UCS blades are configured separately using MAC pinning.

Note You may need to choose a vSwitch policy if both of the following are true:

- The ESXi servers hosting vSwitches are connected to the leaf through a Layer 2 switch or blade server.
- The network requires that the interface group policies between the Layer 2 device and the vSwitch hosted by the ESXi server be different from the interface group policies between the Layer 2 switch and leafs. The policies include Port Channel, Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), Spanning Tree Protocol (STP), and Firewall.

Before you begin

- Before you create a custom attachable entity profile, you must create a VMware vCenter domain. See the section Create a VMM Domain Profile for Cisco ACI Virtual Edge , on page 82 in this guide for more information.

  Note When you create a vCenter domain, you must select an attachable entity profile. However, because you do not have one yet, leave the **Attachable Entity Profile** field blank, or choose default. After you create the custom profile, you can associate it with the vCenter domain.

- Ensure that under **Fabric** > **Access Policies** > **Interfaces** > **Leaf Interfaces** > **Profiles**, the desired interface profiles with port selectors have been created. You associate the ports with the override polices later.
- You must have a vSwitch policy configured for your vCenter domain.

Procedure

Step 1 Log in to the Cisco APIC.

Step 2 Choose **Fabric** > **Access Policies**.

Step 3 In the **Policies** navigation pane, expand the **Policies** and **Global** folders, right-click the **Attachable Access Entity Profiles** folder, and then choose **Create Attachable Access Entity Profile**.

Step 4 In the **Create Attachable Access Entity Profile, Step 1 > Profiles** dialog box, complete the following actions:

a) In the **Name** field, enter a name for the profile.
b) Check the **Enable Infrastructure VLAN** check box.
c) Click the **+** icon to expand **Domains**, and add the VMM domain to be associated with the attachable entity profile.
d) Click **Update**.
e) Click **Next**.

Step 5 In the **Create Attachable Access Entity Profile, Step 2> Association to Interfaces** dialog box, choose the interface policy groups that you want to associate with the attachable entity profile.

Note For each interface policy group, you can choose either the **All** or the **Specific** radio button. The **All** radio button associates all the interfaces from that interface policy group with the attachable entity profile. The **Specific** radio button associates specific interfaces from a specific node. If you choose a **Specific** radio button for an interface policy group, you will be asked to specify the switch IDs and Interfaces and then click an **Update** button.

Step 6 Click **Finish**.

Step 7 Go to **Virtual Networking** > **Inventory**

Step 8 In the left navigation pane, expand the **VMM Domains** and **VMware** folders, and then choose the relevant VMM domain.

Step 9 In the work pane, click the **VSwitch Policy** tab.

Step 10 From the appropriate vSwitch policy drop-down list, choose the policy that you want to apply as an override policy.

Step 11 Click **Submit**.

Create a VMM Domain Profile for Cisco ACI Virtual Edge

Before you can install Cisco Application Centric Infrastructure (ACI) Virtual Edge, you must create a VMM domain for it in Cisco Application Policy Infrastructure Controller (APIC).

Note Use this procedure to configure uplinks for the Cisco ACI Virtual Edge endpoint groups. You cannot configure the uplinks when you create the Cisco ACI Virtual Edge VMM domain using the configuration wizard under the **Fabric** tab. However, if you have already created the Cisco ACI Virtual Edge, you can still add uplinks. See the procedure "Edit the VMM Domain and Modify the Uplinks" in the *Cisco ACI Virtualization Guide, Release 4.2(x)*.

Before you begin

- Ensure that the multicast IP address pool has enough multicast IP addresses to accommodate the number of EPGs to be published to the VMware vCenter domain. You can add more IP addresses to a multicast address pool that is already associated with a VMware vCenter domain at any time.

- Ensure that you have enough VLAN IDs. If you do not, ports EPGs might report that no encapsulation is available.
- Ensure that VMware vCenter is installed, configured, and reachable through the in-band/out-of-band management network.
- Ensure that you have the administrator/root credentials to the VMware vCenter.
- Create interface and switch profiles. See the section "Creating Port Channel Switch and Interface Profiles" in this guide for instructions.
- (Optional) Create an attachable entity profile (AEP).

  During the procedure to create a vCenter domain profile, you are asked to choose or create an AEP. If you want to create one ahead of time, follow the procedure "Configuring an Attachable Entity Profile Using the GUI" in the Cisco ACI Virtual Edge Configuration Guide.

Note Enable the infrastructure VLAN within the AEP assigned to the Cisco ACI Virtual Edge VMM domain. Do this regardless of whether you create the AEP before or during VMware vCenter domain profile creation. In the **Create Attachable Access Entity Profile** dialog box, check the **Enable Infrastructure VLAN** check box.

Procedure

Step 1 Log in to Cisco APIC.

Step 2 Go to **Virtual Networking** > **Inventory**.

Step 3 In the Inventory navigation pane, expand **VMM Domains**, right-click **VMware**, and then choose **Create vCenter Domain**.

Step 4 In the **Create vCenter Domain** dialog box, complete the following steps:

a) In the **Virtual Switch Name** field, enter a name.

b) In the **Virtual Switch Area**, choose **Cisco AVE**.

Choosing **Cisco AVE** creates the VMM domain for Cisco ACI Virtual Edge.

Note Perform the following two substeps if you want to use VMware vSphere Proactive HA. Cisco APIC tells VMware vCenter to quarantine a host with a nonworking Cisco ACI Virtual Edge and move the VMs to a host with a working Cisco ACI Virtual Edge. The feature is not available for Cisco ACI Virtual Edge when it is part of Cisco ACI vPod.

You also must enable Proactive HA in VMware vCenter. See the appendix Improving Cisco ACI Virtual Edge Availability with VMware vSphere Proactive HA, on page 87 in this guide.

c) With the **AVE Time Out Time (seconds)** selector, choose the time period to trigger VMware vCenter to quarantine a host with a nonworking Cisco ACI Virtual Edge and move VMs from the host.

You can choose any value between 10 and 300 seconds, inclusive. The default is 30 seconds.

d) Check the **Host Availability Assurance** check box.

Checking the check box creates a VMware Proactive HA object in VMware vCenter. The object enables VMware vCenter to quarantine a host with a nonworking Cisco ACI Virtual Edge and move VMs from the host.

Note Activation of VMware Proactive HA in vCenter is required before a host with nonworking Cisco ACI Virtual Edge can be quarantined.

e) In the **Switching Preference** area, choose **No Local Switching** or **Local Switching**.

For information about switching preferences, see the section What Cisco ACI Virtual Edge Is, on page 3 in the *Overview* chapter of this guide.

Note If you choose **No Local Switching**, you can use only VXLAN encapsulation.

f) If you chose **Local Switching** in Step 4f, in the **Default Encap Mode** area, choose a mode.

You can choose **VLAN mode** or **VXLAN mode**. You can use both encapsulation methods within the same VMM domain. See the section "Mixed-Mode Encapsulation Configuration" in the Cisco ACI Virtual Edge Configuration Guide.

g) From the **Associated Attachable Entity Profile** drop-down list, create or choose a profile that you created earlier.

See "Configuring an Attachable Entity Profile Using the GUI" in the Cisco ACI Virtual Edge Configuration Guide for instructions.

h) From the VLAN Pool drop-down list, choose or create a VLAN pool.

If Cisco ACI Virtual Edge will be deployed in mixed-mode or VLAN mode, create two VLAN pools: one for primary encapsulation and one for private VLAN implementation. The role for the private VLAN pool must be internal. If Cisco ACI Virtual Edge will be deployed in VXLAN mode, only a private VLAN pool is necessary.

i) In the **AVE Fabric-Wide Multicast Address** field, enter an address.

j) From the **Pool of Multicast Addresses (one per-EPG)** drop-down list, choose or create a pool.

k) In the **vCenter Credentials** area, click the **+** (plus) icon, and in the **Create vCenter credential** dialog box, do the following: Enter the VMware vCenter account profile name in the **Name** field, the VMware vCenter username in the **Username** field, enter and confirm the VMware vCenter password, and then click **OK**.

l) In the **vCenter** area, click the **+** (plus) icon, and in the **Create vCenter Controller** dialog box, do the following: Enter the VMware vCenter controller name, the VMware vCenter host name or IP address, the DVS version, data center name (which must match the data center name configured in VMware vCenter), select the credentials created in the previous step, and then click **OK**.

You can choose a DVS version 5.5 or later.

Note You can create multiple vCenter controllers in the same domain. If you want to create more vCenter controllers, repeat this substep for each new vCenter controller.

m) In the **Create vCenter Domain** dialog box, click **Submit**.

In the VMware work pane, you should see the newly created VMM domain, which will be pushed to VMware vCenter.

n) From the **Number of Uplinks** drop-down list, choose the umber of uplinks to the virtual switch uplink port group.

You can choose to associate up to 32 uplinks to the virtual switch uplink port group. This step is optional; if you do not choose a value, eight uplinks are associated with the port group by default. You can name

Alternate Procedures for Creating vCenter Domain, Interface, and Switch Profiles

the uplinks after you finish creating the VMM domain. You can also configure failover for the uplinks when you create or edit the VMM domain association for an EPG.

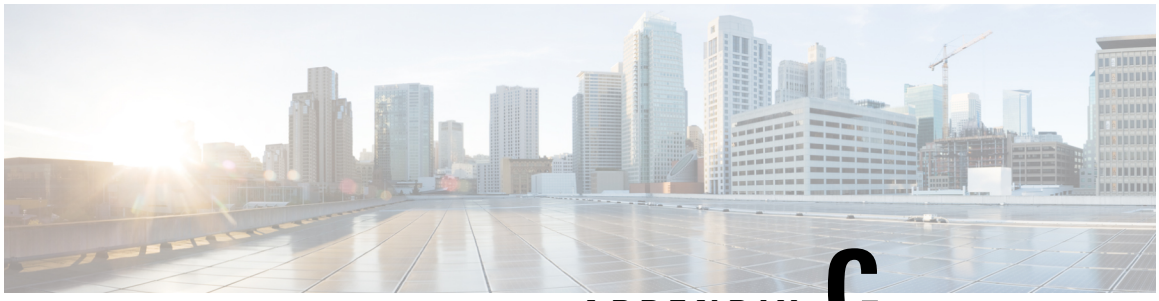
o) Configure the **Port Channel Mode**, **vSwitch Policy**, and other features as appropriate to your setup.

The port channel policy inside the vSwitch policy should be configured correctly, matching the supported topology requirement.

What to do next

- Add one or more ESXi hosts and their PNICs to the newly created Cisco ACI Virtual Edge DVS using the vSphere Web Client on the VMware vCenter.
- Enable vSphere Proactive HA in VMware vCenter if you have not done so already.
- Rename the uplinks or configure failover for them.

Alternate Procedures for Creating vCenter Domain, Interface, and Switch Profiles



APPENDIX C

Improving Cisco ACI Virtual Edge Availability with VMware vSphere Proactive HA

Improving Cisco ACI Virtual Edge Availability

You can use VMware vSphere Proactive HA in vCenter 6.5 and later to improve Cisco ACI Virtual Edge availability.

Cisco Application Policy Infrastructure Controller (APIC) and VMware work together to detect a nonworking Cisco ACI Virtual Edge, isolate its host, and move its virtual machines (VMs) to a working host. Otherwise, if Cisco ACI Virtual Edge crashes, all its VMs can lose network connectivity.

You enable and configure vSphere Proactive HA in VMware vCenter, and in Cisco APIC, where the feature is called **Host Availability Assurance**. You can specify the amount of time that Cisco ACI Virtual Edge is not working before its host is quarantined and its VMs are moved.

Note

- Permission of the Cisco APIC account that you use for registration on VMware vCenter must have administrator rights or right to access the Cisco Application Centric Infrastructure (ACI) vCenter plug-in.
- vSphere Proactive HA is not available for Cisco ACI Virtual Edge when it is part of Cisco ACI Virtual Pod.
- For Host Availability Assurance to work, the VMware vCenter account used to create the Cisco APIC vCenter domain must have "Health Provider" write permission on the VMware vCenter.

Improving Cisco ACI Virtual Edge Availability with VMware vSphere Proactive HA

How Improving Availability with vSphere Proactive HA Works

When you enable Host Availability Assurance, Cisco APIC creates a vSphere Proactive HA provider object in VMware vCenter. The object enables VMware vCenter to quarantine a host with a nonworking Cisco ACI Virtual Edge and move VMs out of that host. In Cisco APIC, you also specify how aggressively you want to trigger quarantine. You perform these tasks when you create a vCenter domain for Cisco ACI Virtual Edge.

When Host Availability Assurance is configured and enabled, Cisco APIC monitors Cisco ACI Virtual Edge on VMware vCenter. It uses the VMware vCenter inventory and OpFlex status to determine if Cisco ACI Virtual Edge is in a good or bad state. If Cisco APIC detects that Cisco ACI Virtual Edge is in a bad state, it tells VMware vCenter to put the affected host into quarantine.

VMware vCenter puts a host in quarantine mode according to one of three remediation modes, which you configure for the cluster:

- **Quarantine**: Hosts with health at yellow and red levels are put into quarantine mode.

Note In Cisco ACI Virtual Edge Release 2.1(1), you can ensure that VM groups are moved out of Cisco ACI Virtual Edge hosts when the hosts stop working. The configuration overrides any affinity groups that would otherwise keep the VMs with particular hosts. For more information, see the section *VM Group Quarantine Protection*, in this guide.

- **Mixed**: Hosts with health at the yellow level are put into quarantine mode; hosts with health at the red level are put into maintenance mode.

Note Although you can choose mixed remediation mode in VMware vCenter, the resulting behavior is the same as quarantine remediation mode.

- **Maintenance**: Hosts with health at yellow and red levels are put into maintenance mode.

Important Do not choose maintenance mode remediation when you use vSphere Proactive HA. Maintenance mode requires that Cisco ACI Virtual Edge be powered off, which prevents the host from ever returning to a healthy state. Only use quarantine or mixed mode.

VMware vCenter also moves the VMs on that host to a host with a working Cisco ACI Virtual Edge. However, hosts in quarantine still might run data VMs if no healthy host is available, and any VM pinned by Distributed Resource Scheduler (DRS) rules to a quarantined host stays on the host. VMware vCenter also avoids moving any VMs to a quarantined host. However, you can deploy new VMs on a host in quarantine.

Benefits of Using vSphere Proactive HA

Using the vSphere Proactive HA feature is how you can detect and react to a Cisco Application Centric Infrastructure (ACI) Virtual Edge failure. If Cisco ACI Virtual Edge goes down, all of its virtual machines (VMs) that are connected to a VMware vCenter portgroup with **AVE** switching mode lose network connectivity.

vSphere Proactive HA also can prevent loss of connectivity in the following situations:

- **vSphere DRS**: The load-balancing vSphere Distributed Resource Scheduler (DRS) feature uses vSphere vMotion to automatically move VMs to enforce behavior that you define though affinity rules.

  However, DRS does not take Cisco ACI Virtual Edge into account. So in optimizing CPU and memory utilization, it can migrate a VM from a host with a working Cisco ACI Virtual Edge to a host where Cisco ACI Virtual Edge is not working.

- **Going into maintenance mode**: When you put a host into maintenance mode, DRS automatically migrates all of the host's VMs to another host. The host enters maintenance mode after all the VMs are moved.

  However, because Cisco ACI Virtual Edge is pinned to the host, DRS does not move Cisco ACI Virtual Edge, so the host doesn't enter maintenance mode. So without vSphere Proactive HA, you must power off the Cisco ACI Virtual Edge host for it to enter maintenance mode.

- **Going out of maintenance mode**: When you take a host out of maintenance mode, DRS can migrate VMs to that host because all of its CPU and memory are again available. However, Cisco ACI Virtual Edge must be powered on manually. This means that the Cisco ACI Virtual Edge might not be ready before DRS starts moving VMs back to the host.

  But vSphere Proactive HA lets Cisco ACI Virtual Edge power up on its own and delay moving VMs to the host until it is ready.

Important The host automatically enters and exits maintenance mode only in Cisco ACI Virtual Edge 2.1(1a) and later releases only. Earlier releases require that you put the host into and take it out of maintenance mode manually when using vSphere Proactive HA.

How vSphere Proactive HA Works

You enable and configure vSphere Proactive HA in VMware vCenter and in Cisco Application Policy Infrastructure Controller (APIC), where the feature is called **Host Availability Assurance**.

Enabling and configuring vSphere Proactive HA feature creates a vSphere Proactive HA provider object in VMware vCenter. The object enables VMware vCenter to quarantine a host with a nonworking Cisco ACI Virtual Edge and move VMs out of that host.

The feature also assigns a health status—green, yellow, or red—to every ESXi host in a Cisco ACI Virtual Edge virtual machine manager (VMM) domain. The status is green if the Cisco ACI Virtual Edge distributed virtual switch (DVS) is not added to the host or if the DVS is added and OpFlex is online. the status is yellow if the DVS is added and OpFlex is offline.

You also can specify how aggressively you want to trigger quarantine for the hosts.

Improving Cisco ACI Virtual Edge Availability with VMware vSphere Proactive HA

Once you enable and configure vSphere Proactive HA, Cisco APIC and VMware vCenter work together to detect and isolate a nonworking Cisco ACI Virtual Edge.

1. Cisco APIC monitors Cisco ACI Virtual Edge on VMware vCenter.

   It uses the VMware vCenter inventory and OpFlex status to determine if Cisco ACI Virtual Edge is in a good or bad state. If Cisco APIC detects that Cisco ACI Virtual Edge is in a bad state, it tells VMware vCenter to put the affected host into quarantine by using the yellow level.

2. VMware vCenter puts a host in quarantine mode according to a remediation mode, which you configure for the cluster in VMware vCenter:

   Note Red status exists in VMware vCenter; it does not exist in Cisco APIC.

   - **Quarantine**: Hosts with health at yellow and red levels are put into quarantine mode.

     Note In a Proactive HA cluster, VMware vCenter does not move a Cisco ACI Virtual Edge host into quarantine even if OpFlex goes down when an uplink or a physical network interface card (PNIC) is removed from the host.

   - **Mixed**: Hosts with health at the yellow level are put into quarantine mode; hosts with health at the red level are put into maintenance mode.

     Note Although you can choose mixed remediation mode in VMware vCenter, the resulting behavior is the same as quarantine remediation mode.

     Note Do not choose maintenance mode remediation when you use vSphere Proactive HA. Maintenance mode requires that Cisco ACI Virtual Edge be powered off, preventing the host from ever returning to a healthy state. Use only quarantine or mixed remediation mode.

3. VMware Distributed Resource Scheduler (DRS) moves the VMs on the nonworking host to a host with a working Cisco ACI Virtual Edge.

   Note Hosts in quarantine still might run data VMs if no healthy host is available, and any VM pinned by DRS rules to a quarantined host stays on the host. VMware vCenter also avoids moving any VMs to a quarantined host. However, you can deploy new VMs on a host in quarantine.

Note In Cisco ACI Virtual Edge Release 2.1(1) and later, you can ensure that VM groups are moved out of Cisco ACI Virtual Edge hosts when the hosts stop working. The configuration overrides any affinity groups that would otherwise keep the VMs with particular hosts. For more information, see and later the section VM Group Quarantine Protection, on page 94 in this guide.

4. Cisco APIC watches VMware vCenter events for hosts entering maintenance mode or rebooting and powers off Cisco ACI Virtual Edge when it is the only powered-on VM left on the host.
5. Cisco APIC powers on Cisco ACI Virtual Edge when the host is rebooted or taken out of maintenance mode.

Prerequisite for Configuring VMware vSphere Proactive HA

Complete the following task before you configure VMware vSphere Proactive HA.

Make sure that the VMware vCenter account used to create the Cisco APIC vCenter domain has "Health Provider" write permission on the VMware vCenter.

Enabling vSphere Proactive HA in Cisco APIC

Improving Cisco Application Centric Infrastructure (ACI) Virtual Edge in Cisco Application Policy Infrastructure Controller (APIC) consists of the following tasks:

- Enabling host availability assurance on the Cisco Application Centric Infrastructure (ACI) Virtual Edge VMM domain
- Specifying the time period before VMware vCenter quarantines any hosts on with Cisco ACI Virtual Edge has stopped working

You can perform these tasks in the Cisco APIC GUI when you create a vCenter domain for Cisco ACI Virtual Edge. See the section Create a VMM Domain Profile for Cisco ACI Virtual Edge , on page 82 in this guide for instructions.

You can perform these tasks with the NX-OS style CLI and REST API instead of the Cisco APIC GUI. See the sections Enabling vSphere Proactive HA Using NX-OS Style CLI, on page 96 and Enabling vSphere Proactive HA Using REST API, on page 101 in this guide.

Note When you add hosts to a cluster on which Proactive HA is already configured, and then add the host or attach the host to a Cisco ACI Virtual Edge VMM domain, those hosts may not work properly in some circumstances. The hosts may not work properly in Proactive HA or when Cisco ACI Virtual Edge or OpFlex goes down. The hosts also may not go into quarantine mode although the health status of the host is correctly set to yellow in Cisco Cisco Application Policy Infrastructure Controller (APIC).

To fix the problem, disable Proactive HA on the cluster and then re-enable it.

Enabling vSphere Proactive HA in VMware vCenter

Before you begin

Using vSphere Proactive High Availability (HA) requires VMware vCenter 6.5 or later.

Note When you add hosts to a cluster on which Proactive HA is already configured, and then add the host or attach the host to a Cisco Application Centric Infrastructure (ACI) Virtual Edge VMM domain, those hosts may not work properly in some circumstances. The hosts may not work properly in Proactive HA or when Cisco ACI Virtual Edge or OpFlex goes down. The hosts also may not go into quarantine mode although the health status of the host is correctly set to yellow in Cisco Cisco Application Policy Infrastructure Controller (APIC).

To fix the problem, disable Proactive HA on the cluster and then re-enable it.

Procedure

Step 1 Log in to the VMware vCenter Web Client.

Step 2 Choose **Home** > **Host and Cluster** > ***cluster*** > **Configure** > **Edit**.

Step 3 In the **Edit Cluster Settings** dialog box, choose **vSphere Availability** in the left navigation pane and then check the **Turn on Proactive HA** check box in the work pane.

Step 4 In the left navigation pane, choose **Proactive HA Failures and Responses**complete the following steps:

a) From the **Remediation** drop-down list, choose a remediation level.

Choose either **Quarantine**, which puts hosts with yellow and red levels into quarantine mode or **Mixed**, which puts yellow hosts into quarantine mode and red hosts into maintenance mode.

Note Do not choose **Maintenance**, which puts yellow and red hosts into maintenance mode. Maintenance mode requires that Cisco ACI Virtual Edge be powered off, which prevents the host from ever returning to a healthy state

b) Check the check box next to the vSphere Proactive HA provider to enable it.

The Cisco Application Policy Infrastructure Controller (APIC)-created provider would have "vmm-domain-name_APIC" as its name.

Manually Setting the Health Level of the ESXi Host

By default, the state of the VMware host is determined by the state of the Cisco Application Centric Infrastructure (ACI) Virtual Edge that resides on it.

You might want to override the default if you must do maintenance on the Cisco Application Centric Infrastructure (ACI) Virtual Edge. Setting the host state to yellow or red while Cisco ACI Virtual Edge is working properly puts the corresponding host into quarantine mode.

Or you might not want a specific host to go into quarantine, even if the Cisco ACI Virtual Edge on it goes down. Setting the state to green keeps the host active, disabling vSphere Proactive HA on the host.

Setting the health state manually to green prevents Cisco Application Policy Infrastructure Controller (APIC) from changing host status to yellow or red. You can view and set the health state using the Cisco APIC GUI, NX-OS style CLI, or REST API. See the section "Viewing and Setting a State on the Cisco ACI Virtual Edge Host Using the Cisco APIC GUI, on page 93." You also can view host health status and events in VMware vCenter. See "Tracking Health Updates for a Host in VMware vCenter, on page 93."

Viewing and Setting a State on the Cisco ACI Virtual Edge Host Using the Cisco APIC GUI

Before you begin

- You must have a host that contains Cisco ACI Virtual Edge.
- Host Availability Assurance must be enabled for the VMM domain on Cisco Application Policy Infrastructure Controller (APIC).

Procedure

Step 1 Log in to Cisco APIC.

Step 2 Go to **Virtual Networking** > **Inventory** > **VMM Domains** > **VMware** > ***VMM domain*** > **Controllers** and click the controller.

Step 3 In the **Controller Instance** work pane, in the **Health Policy** area, click the + (plus icon).

Step 4 Enter the host IP address and choose the state from the drop-down list, and then click **Update**.

Step 5 Click **Submit**.

Tracking Health Updates for a Host in VMware vCenter

If you enable Proactive HA, you can view events in VMware vCenter to track health updates for a host.

Procedure

Step 1 Log in to the VMware vCenter Web Client.

Step 2 Navigate to the host.

Step 3 In the central work pane, click the **Monitor** tab, **Tasks & Events**, and then **Events**.

The **Description** pane displays events for the host. In the **Type** column, VMware vCenter gives a warning for changes in the host's health, such as a degraded status or the host's subsequently entering a quarantine mode. There can be a 30-second delay between the report of a health problem and the host's being put into a different mode.

VM Group Quarantine Protection

When you enable Host Assurance Availability, the virtual machine (VM) reamains available even if Cisco Application Centric Infrastructure (ACI) Virtual Edge fails. Host Assurance Availability causes Cisco APIC to trigger the vMotion of VMs by setting the health status of the ESXi host where Cisco ACI Virtual Edge is in nonworking state to yellow or red.

However, Distributed Resource Scheduler (DRS) affinity rules and load balancing settings can cause VMs to stay or be placed on a nonworking host. Configuring protected VM groups enables Cisco APIC to autocreate anti-affinity rules in VMware vCenter, which force VMs part of the group to move out of nonworking host.

To protect VM groups, you must create the VM groups in VMware vCenter and enable protection for those VM groups in Cisco APIC. Each VM group should have all VMs that use Cisco ACI Virtual Edge.

You configure VM group protection in Cisco Application Policy Infrastructure Controller (APIC) on specific controllers. You can use the Cisco APIC GUI, NX-OS style CLI, or REST API.

Note For VM group quarantine protection to work, the VMware vCenter account used to create the Cisco APIC vCenter domain must have write privileges on the "Cluster" object in VMware vCenter.

Configuring VM Group Protection Using the Cisco APIC GUI

You can use the Cisco APIC GUI to configure VM group protection.

Before you begin

You must have configured VM groups in VMware vCenter and enabled vSphere Proactive HA in Cisco Application Policy Infrastructure Controller (APIC).

Procedure

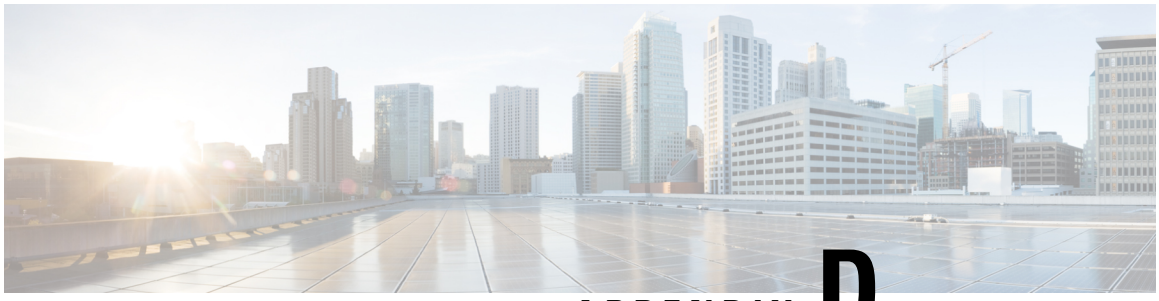
Step 1 Log in to Cisco APIC.

Step 2 Go to **Virtual Networking** > **Inventory** > **VMM Domains** > **VMware** > ***domain*** > **Controllers** > ***controller***.

Step 3 In the controller work pane, choose the **Policy** and **General** tabs.

Step 4 In the **Protected VM Groups** area, check the check box for one or more VM groups.

Step 5 Click **Submit**.



APPENDIX D

Performing Tasks Using the NX-OS Style CLI

Migration to Cisco ACI Virtual Edge

Migrate a VDS Domain to Cisco ACI Virtual Edge Using the NX-OS Style CLI

During migration, you enable the domain to use Cisco ACI Virtual Edge.

Before you begin

You have created a VDS domain. See the procedure "Creating a VMM Domain Profile" in the *Cisco ACI Virtualization Guide*.

Procedure

Migrate the VDS VMM domain.

Example:

```
apic1(config)# vmware-domain mininet
apic1(config-vmware)# configure-ave
apic1(config-vmware-ave)# vxlan multicast-pool 225.2.1.1-225.2.1.100
apic1(config-vmware-ave)# exit
apic1(config-vmware)# exit
apic1(config)# exit
apic1#
```

Improving Cisco ACI Virtual Edge Availability with VMware vSphere Proactive HA

Enabling vSphere Proactive HA Using NX-OS Style CLI

You can use the NX-OS style CLI to perform several tasks in Cisco Application Policy Infrastructure Controller (APIC):

- Enable host availability assurance, which creates a vSphere Proactive HA provider object that resides in VMware vCenter. The object enables VMware vCenter to quarantine a host with a nonworking Cisco Application Centric Infrastructure (ACI) Virtual Edge and move its VMs.
- Set the time period before VMware vCenter quarantines the host with the nonworking Cisco ACI Virtual Edge and move VMs from the host.

Note When you add hosts to a cluster on which Proactive HA is already configured, and then add the host or attach the host to a Cisco ACI Virtual Edge VMM domain, those hosts may not work properly in some circumstances. The hosts may not work properly in Proactive HA or when Cisco ACI Virtual Edge or OpFlex goes down. The hosts also may not go into quarantine mode although the health status of the host is correctly set to yellow in Cisco Cisco Application Policy Infrastructure Controller (APIC).

To fix the problem, disable Proactive HA on the cluster and then re-enable it.

Procedure

Step 1 Enable host availability assurance:

```
apic1# config
apic1(config)# vmware-domain mininet
apic1(config-vmware)# avail-monitor enable
apic1(config-vmware)# show run
# Command: show running-config vmware-domain mininet
# Time: Mon Aug  6 22:05:58 2018
  vmware-domain mininet
    vlan-domain member mininet type vmware
    vcenter 172.23.143.235 datacenter mininet dvs-version 6.0
      # username admin
      esx-avail-override 172.23.143.228 yellow
      exit
    configure-ave
      switching mode vxlan
      multicast-address 225.1.1.1
      vxlan multicast-pool 225.2.1.1-225.2.1.100
      exit
    avail-monitor enable
    exit
apic1(config-vmware)#
```

Step 2 Set the Cisco ACI Virtual Edge timeout:

```
apic1# config
apic1(config)# vmware-domain mininet
apic1(config-vmware)# configure-ave
apic1(config-vmware-ave)# ave-timeout 10
```

You can choose any value between 10 and 100 seconds, inclusive. The default is 30 seconds.

What to do next

Enable the VMware vSphere Proactive HA feature in VMware vCenter if you have not done so already. See the section Enabling vSphere Proactive HA in VMware vCenter, on page 92 in this guide.

You can set a state for a given host to override the default state, which is based on the health of the Cisco ACI Virtual Edge. See the section Manually Setting the Health Level of the ESXi Host, on page 92.

Setting a State on the Cisco ACI Virtual Edge Host Using NX-OS Style CLI

Before you begin

You must have a host that contains Cisco ACI Virtual Edge.

Procedure

Set a state for the host:

```
apic1# config
apic1(config)# vmware-domain mininet
apic1(config-vmware)# vcenter 192.168.0.235 datacenter apic1(config-vmware)# vcenter
172.23.143.235 datacenter mininet
apic1(config-vmware-vc)# esx-avail-override 192.168.0.1 yellow
apic1(config-vmware-vc)# show run
# Command: show running-config vmware-domain mininet vcenter 192.168.0.235 datacenter
 mininet
# Time: Mon Aug  6 23:47:17 2018
  vmware-domain mininet
    vcenter 192.168.0.235 datacenter mininet dvs-version 6.0
      # username admin
      esx-avail-override 192.168.0.1 yellow
      exit
    exit
apic1(config-vmware-vc)#
```

Configuring VM Group Protection Using the NX-OS Style CLI

You can use the NX-OS style CLI to guarantee that specific VM groups be moved to working hosts if a Cisco Application Centric Infrastructure (ACI) Virtual Edge host stops working.

Before you begin

You must have configured VM groups in VMware vCenter and enabled vSphere Proactive HA in Cisco Application Policy Infrastructure Controller (APIC).

Performing Tasks Using the NX-OS Style CLI

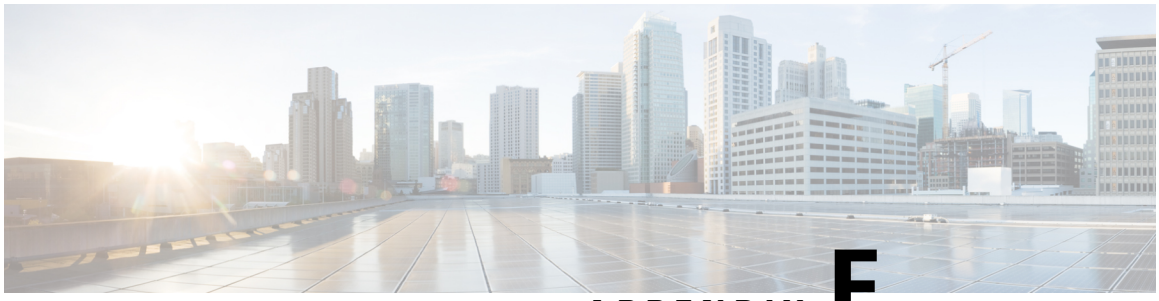
Procedure

Configure VM group protection.

Example:

```
apic1# config
apic1(config)# vmware-domain mininet
apic1(config-vmware)# vcenter 192.168.0.1 datacenter mininet
apic1(config-vmware-vc)# protect-vm-group "AVE_Cluster_Name/VM_Group_Name"
```

AVE_Cluster_Name is the name of the ESXi cluster on the VMware vCenter where the VM groups have been defined and where the affinity rules are programmed. VM groups are cluster-specific. *VM_Group_Name* is the name of the VM group present in the specified cluster.



APPENDIX E

Performing Tasks Using REST API

Migration to Cisco ACI Virtual Edge

Migrate the Cisco AVS VMM Domain to Cisco ACI Virtual Edge Using REST API

A VMM domain must be ready for the hosts and VMs before you migrate from Cisco AVS to Cisco ACI Virtual Edge. You can use REST API to migrate the VMM domain. This is easier than creating a new VMM domain, which requires that you manually reproduce most of the configuration of the Cisco AVS domain.

Note You can migrate only one Cisco AVS VMM domain at a time.

Procedure

Migrate the Cisco AVS VMM domain, providing its name, the name of the Cisco ACI Virtual Edge domain that you want to create, and user account information.

You must provide the user account information—the username and password—for the previous Cisco AVS. It is optional to specify a new VLAN pool.

Example:

The following example migrates a Cisco AVS domain named `prod-avs` to a domain named `ave`. It also creates a new VLAN pool for the Cisco ACI Virtual Edge domain.

```
{{ifc}}/mqapi2/migrateVMwareDomain.xml?name=prod-avs
<vmmDomP dn="uni/vmmp-VMware/dom-ave" name="ave" enableAVE="true" >
 <vmmUsrAccP name="adminAcc" usr="administrator@vsphere.local" pwd="In$1eme1" />
 <infraRsVlanNs tDn="uni/infra/vlanns-[inst_pvlan]-dynamic"/>
</vmmDomP>
```

By default, all EPGs from the Cisco AVS domain are automatically associated with the new domain. If you do not want to associate the EPGs, add the parameter `migrateEPGs=False`.

Associating the EPGs from the Cisco AVS domain to the new Cisco ACI Virtual Edge domain does not remove the old association.

What to do next

Follow instructions in the section Migrate from Cisco AVS to Cisco ACI Virtual Edge Using the Cisco ACI vCenter Plug-in, on page 46 in this guide.

Migrate a VDS Domain to Cisco ACI Virtual Edge Using REST API

Before you begin

You have created a VDS domain. See the procedure "Creating a VMM Domain Profile" in the *Cisco ACI Virtualization Guide*.

Procedure

Step 1 Create a multicast address pool if you have not done so.

Example:

```
<polUni>
<infraInfra>
    <fvnsMcastAddrInstP name="mcast1">
            <fvnsMcastAddrBlk name="mcastrange" from="225.2.1.1" to="225.2.1.100"/>
    </fvnsMcastAddrInstP>
</infraInfra>
</polUni>
```

Step 2 Set `enableAVE=true` on the VMM domain and associate the multicast address pool with it.

Example:

```
<polUni>
<vmmProvP vendor="VMware">
    <vmmDomP name="mininet" enableAVE="true">
        <vmmRsDomMcastAddrNs tDn="uni/infra/maddrns-mcast1"/>
   </vmmDomP>
</vmmProvP>
</polUni>
```

Improving Cisco ACI Virtual Edge Availaility with VMware vSphere Proactive HA

Enabling vSphere Proactive HA Using REST API

You can use REST API to perform several tasks in Cisco Application Policy Infrastructure Controller (APIC):

- Enable host availability assurance, which creates a vSphere Proactive HA provider object that resides in VMware vCenter. The object enables VMware vCenter to quarantine a host with a nonworking Cisco Application Centric Infrastructure (ACI) Virtual Edge and move its VMs.
- Set the time period before VMware vCenter quarantines the host with the nonworking Cisco ACI Virtual Edge and move VMs from the host.

Note When you add hosts to a Cisco ACI Virtual Edge cluster on which Proactive HA is already configured, and then add the host or attach the host to a Cisco ACI Virtual Edge VMM domain, those hosts may not work properly in some circumstances. The hosts may not work properly in Proactive HA or when Cisco ACI Virtual Edge or OpFlex goes down. The hosts also may not go into quarantine mode although the health status of the host is correctly set to yellow in Cisco Cisco Application Policy Infrastructure Controller (APIC).

To fix the problem, disable Proactive HA on the cluster and then re-enable it.

Procedure

Step 1 Enable host availability assurance:

```
{{ifc}}/api/node/mo/.xml
<polUni>
  <vmmProvP vendor="VMware”  >
      <vmmDomP name="mininet" hvAvailMonitor=”yes”>
 </vmmDomP>
  </vmmProvP>
</polUni>
```

Step 2 Set the Cisco ACI Virtual Edge timeout:

```
{{ifc}}/api/node/mo/.xml
<polUni>
  <vmmProvP vendor="VMware">
      <vmmDomP name="mininet” aveTimeOut=”10">
      </vmmDomP>
  </vmmProvP>
</polUni>
```

You can choose any value between 10 and 100 seconds, inclusive. The default is 30 seconds.

What to do next

Enable the VMware vSphere Proactive HA feature in VMware vCenter if you have not done so already. See the section Enabling vSphere Proactive HA in VMware vCenter, on page 92 in this guide.

You can set a state for a given host to override the default state, which is based on the health of the Cisco ACI Virtual Edge. See the section Manually Setting the Health Level of the ESXi Host, on page 92.

Setting a State on the Cisco ACI Virtual Edge Host Using REST API

Before you begin

You must have a host that contains Cisco ACI Virtual Edge.

Procedure

Set a state for the host:

```
{{ifc}}/api/node/mo/.xml
<polUni>
  <vmmProvP vendor="VMware">
      <vmmDomP name="mininet">
         <vmmCtrlrP name="vc65.xyz.com">
        <vmmHvAvailPol>
       <vmmHvDesiredSt host=”172.23.143.228" state="yellow"/>
        </vmmHvAvailPol>
         </vmmCtrlrP>
     </vmmDomP>
  </vmmProvP>
</polUni>
```

Configuring VM Group Protection Using REST API

You can use REST API to guarantee that specific VM groups be moved to working hosts if a Cisco Application Centric Infrastructure (ACI) Virtual Edge host stops working.

Before you begin

You must have configured VM groups in VMware vCenter and enabled vSphere Proactive HA in Cisco Application Policy Infrastructure Controller (APIC).

Procedure

Configure VM group protection.

Example:

```
<polUni>
<vmmProvP vendor="VMware">
    <vmmDomP name="mininet"  hvAvailMonitor="true">
     <vmmCtrlrP name="vc65.xyz.com">
      <vmmHvAvailPol>
```

```
       <vmmProtectedVmGroup
tDn="comp/prov-VMware/ctrlr-[mininet]-vc65.xyz.com/hvcluster-domain-c94/vmgroup-vm01"></vmmProtectedVmGroup>

      </vmmHvAvailPol>
     </vmmCtrlrP>
   </vmmDomP>
</vmmProvP>
</polUni>
```

In the preceding example, note the following:

- The tDN property of vmmProtectedVmGroup is the dn property of compVmGroup (vm groups that are pulled from the vCenter inventory).
- The list of compVmGroup can be queried through GET:`https://{apic}/api/node/class/compVmGroup.xml` .

Performing Tasks Using REST API